日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１０月１５日

出願番号
Application Number:　特願２００２－３００１０８

[ST.10/C]:　[ＪＰ２００２－３００１０８]

出願人
Applicant(s):　松下電器産業株式会社

２００３年　７月　１日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０５１９５５

【書類名】　特許願

【整理番号】　2032740087

【提出日】　平成14年10月15日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　杉山　圭司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　▲たか▼尾　直弥

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　グループ検索方法、グループ情報入手方法およびエントリポイント検索方法

【特許請求の範囲】

【請求項１】　検索者がＰ２Ｐネットワーク上に存在するグループに参加するための情報を入手するための検索手段であって、

ネットワーク上に存在するグループを特定するための情報を含むグループ情報を入手するグループ情報入手ステップと、

入手したグループ情報に対応するグループのエントリポイントの情報を入手するエントリポイント入手ステップと、

を実行することを特徴とするグループ検索方法。

【請求項２】　検索者がグループを検索するためのグループ検索メッセージを生成し、

問い合わせを行うグループ情報検索ステップと、

グループ検索メッセージを受け取った応答者が、グループ公開鍵を含むグループ情報を検索者に送信するためのグループ情報応答メッセージを生成し、応答を行うグループ情報応答ステップと、

を実行することを特徴とするグループ情報入手方法。

【請求項３】　前記グループ情報応答ステップにおいて、

グループ管理者が保持するグループ秘密鍵に基づいてグループ情報応答メッセージを生成することを特徴とする第２の請求項記載のグループ情報入手方法。

【請求項４】　前記グループ情報応答ステップにおいて、グループ管理者からグループ参加証発行許可証の発行をうけた発行者が、

グループ参加証発行許可証に含まれる公開鍵に対応する秘密鍵に基づいてグループ情報応答メッセージを生成することを特徴とする第２の請求項記載のグループ情報入手方法。

【請求項５】　検索者がグループ公開鍵を含むグループ情報に基づいてエントリポイント検索メッセージを生成し、

問い合わせを行うエントリポイント検索ステップと、

前記エントリポイント検索メッセージを受信した応答者が受信したエントリポイント検索メッセージに対応するグループのエントリポイントの情報を含むエントリポイント検索応答メッセージを生成し、
応答を行うエントリポイント検索応答ステップと、
を行うことを特徴とするエントリポイント検索方法。

【請求項６】　前記エントリポイント検索応答ステップにおいて、エントリポイント検索メッセージの受信者が、エントリポイント検索メッセージに含まれるグループ公開鍵と応答者が保有するグループ公開鍵の比較によって、検索者の要求しているグループと応答者が所属しているグループの一意性を確認することを特徴とする請求項５記載のエントリポイント検索方法。

【請求項７】　前記エントリポイント検索応答ステップにおいて、エントリポイント検索メッセージの受信者が、エントリポイント検索メッセージに含まれるグループ公開鍵と応答者が保有するグループ公開鍵の比較だけでなく、検索メッセージに含まれるグループ公開鍵が、応答者が保有するグループ公開鍵更新履歴との比較によって、検索者の要求しているグループと応答者が所属しているグループの一意性を確認することを特徴とする請求項５記載のエントリポイント検索方法。

【請求項８】　前記エントリポイント検索応答ステップにおいて、グループの一意性が確認でき、かつエントリポイント検索メッセージに含まれるグループ公開鍵が、応答者の保有する最新のグループ公開鍵でない場合に、最新のグループ公開鍵を通知することを特徴とする請求項７記載のエントリポイント検索方法。

【請求項９】　前記エントリポイント検索応答ステップにおいて、応答者がグループ参加証、および応答者の秘密鍵に基づいてエントリポイント検索応答メッセージを生成することを特徴とする請求項５記載のエントリポイント検索方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークで接続された機器によって構成されるグループに関する情報を取得するための検索方法に関する。

【０００２】

【従来の技術】

インターネットに接続してネットワークサービスを享受するユーザ数は、接続機器や接続料金の廉価化、接続機器の多彩化、および通信速度の向上などにより急速に増加している。インターネット普及当初は、一部の情報提供者が提供する情報を一般ユーザがダウンロードする一方向のサービスが主流であったが、現在は自分の持つ情報、すなわちテキストデータ、静止画像データ、音声データ、動画像データなどを発信したいという。

【０００３】

一般ユーザも増え、主にＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）などのサーバに自分の情報を複製し、他のユーザが閲覧可能とすることによってこれを実現している。

【０００４】

サーバで情報を公開するにあたっては、大きく分けて（１）サーバを自分で運用する、（２）サービス提供者が有料または無料で提供しているサーバに情報をアップロードする、という二つの方法がある。さらに、不特定多数を対象に発信するのではなく、友人・家族・共通の趣味を持つ者など特定ユーザ間（以下グループと呼ぶ）でのみプライベートな情報を共有したいという要求も増えているが、これを実現する方法としては、主に認証サーバを用いる方法、すなわちグループへの参加を認められたユーザのユーザＩＤとパスワードの組（以下グループリスト）を認証サーバ（情報提供サーバと同一であっても良い）に登録しておき、ユーザが入力したユーザＩＤとパスワードの組を確認することによって当該グループでの情報共有を許可する方法などが用いられている。

【０００５】

また、作成したグループを公開する際にも、グループに関する情報、つまりグループのカテゴリやメンバの情報、参加のための条件などを登録サーバに登録することにより、不特定多数のユーザに参加を呼びかけることが多い。ユーザは登録サーバにアクセスすることによって、登録されているグループの存在を知り、グループへの参加に必要な情報を入手する。チャット、ＢＢＳ、メーリングリス

トなどのネットワーク上でのコミュニケーションを行うことを目的とするグループの多くはこのような方法で、グループを公開する。

【０００６】

このように情報提供者はサーバに情報を格納しておき、情報受信者がサーバへアクセスするというモデル（サーバークライアントモデルと呼ぶ）には、次の問題点がある。

【０００７】

すなわち、自分でサーバを運用する場合には、

（１）高度な知識が必要：サーバやネットワーク等に関する十分な知識が必要とされ、一般ユーザが運用することは困難な場合が多い、

（２）コストがかかる：機材やソフトウェア以外にも、基本的に常時サービスを提供するためにサーバを常時稼動させるための運用費が必要となる、

などの問題点があり、有料または無料で提供されるサーバを利用する場合には、

（３）容量制限：多くの場合サーバに格納できる情報の容量には制限が設けられており、有料サーバの場合はコストをより多く負担することで容量制限を緩和することができるが、その場合にはより多くのコストがかかる、

（４）プライバシ：サーバ提供者が信頼に足る場合であっても、何らかの事故等でサーバに格納した情報が第三者に漏れる場合があり、真にプライバシ保護を必要とする情報を共有することは困難である、

などの問題点があり、共通の課題としては、

（５）信頼性：サーバが何らかのトラブルでアクセス不能になった場合、情報発信や情報共有はまったく不可能となる、

という問題点がある。

【０００８】

なお、上で述べたコストに関する問題については、情報提供に対する収入によりコストを回収できるならば一定の負担は問題とならないが、一般ユーザが個人情報を発信あるいは共有する多くの場合はこれに当てはまらない。

【０００９】

上記のようなサーバークライアントモデルにおける情報共有時の問題点を解消

するために近年着目されているのがピアートゥーピア（Ｐｅｅｒ－ｔｏ－Ｐｅｅｒ、以下Ｐ２Ｐ）モデルである。これは、情報をサーバに一極集中させず、必要なときに情報発信者－情報受信者間で直接伝送することで上記問題点を解決するものである（例えば、非特許文献１参照）。

【００１０】

Ｐ２Ｐモデルのネットワーク（以下Ｐ２Ｐネットワーク）に参加しているユーザ間で情報を転送する場合の流れを図１０にて例示する。

【００１１】

各ユーザはＰ２Ｐネットワークに参加している他のユーザの存在を一人以上知っており、例えばＡはＢとＦ、ＢはＡとＣとＤ、ＥはＤのみの存在を知っている。この状態でＡが欲する情報を受信する際には、まず情報を持つユーザを特定するために検索を行う。Ａはまず自分の知っているＢとＦに検索要求を発する。次にＢとＦはそれぞれが知っているユーザにこの検索要求を中継し、その先のユーザも同様に中継する（ステップ１００１）。そして、この検索要求に合致する情報を持っているユーザ、この場合はＣとＥは、Ａに対して情報を持っていることを直接通知し（ステップ１００２）、Ａは何らかの判断基準でＥを選択してＡとＥの間で情報の転送が直接行われる（ステップ１００３）。もちろん情報を分割してＣとＥの両者から同時に転送することも可能である。これにより、前記サーバークライアントモデルの問題点（１）～（５）は次のように解決される。

【００１２】

（１）サーバを運用しないため高度な知識は必要とされない。

【００１３】

（２）またサーバを運用または利用するためのコストも不要である。

【００１４】

（３）情報発信者Ｅから直接情報Ａを受信するので、転送可能な情報の容量はＡとＥのローカルな記録容量のみに制約され、実質的に容量の制限はない。

【００１５】

（４）転送される情報はＡとＥ以外の第三者を経由しないので、既存技術でＡとＥの間の通信路を暗号化するなどすれば情報のプライバシは保たれる。

【００１６】

（５）仮にＥがネットワークに参加していない状態（オフライン）であっても、ＡはＣから必要な情報を得ることができる。

【００１７】

さて、Ｐ２Ｐネットワークにおいてグループでの情報共有を行う場合には登録サーバといった、グループに関する情報を管理しているサーバが存在しないので、グループに参加するユーザは、何らかの別の方法でグループに関する情報を入手する必要がある。

【００１８】

その際には、上記で述べたＰ２Ｐモデルによる情報伝達の手法を用いることができる。グループに関する情報を入手するための検索をＰ２Ｐネットワークによって実行することにより、登録サーバを使用することなく、ネットワーク上に存在するグループの情報を入手することが出来る。

【００１９】

ユーザは、まず

（１）ネットワーク上に存在するグループを識別するための情報および

（２）グループを分類するための属性などに関する情報を入手し、次に

（３）グループの参加するための場所に関する情報

を入手する必要がある。

【００２０】

（１）の情報はグループに与えられたＩＤなどであり、グループを一意に指定できる情報である。

【００２１】

（２）の情報はグループのカテゴリ、活動目的、グループへの参加条件などである。

【００２２】

（３）グループのメンバのＩＰアドレス、ポート番号などであり、実際にグループのメンバにアクセスするために必要な情報である。

【００２３】

本発明では以後（１）の情報をグループ識別情報、（２）の情報をグループ属性情報、（３）の情報をエントリポイント情報と呼ぶ。また、（１）および（２）の情報をまとめたものをグループ情報と呼ぶ。

【００２４】

ユーザはまず、検索によってグループ識別情報および、グループ属性情報を入手し、入手したグループ属性情報から、そのグループに参加するかどうかを判断する。そのグループに参加する場合には、グループのエントリポイント情報を検索によって入手する。この際に、先に入手しているグループ識別情報によって、どのグループのエントリポイントが必要であるのかを指定する。エントリポイント情報を入手したユーザは、該当するエントリポイントにアクセスすることによってグループの活動に参加する。上記の処理をＰ２Ｐネットワークの検索手段を用いて行う場合、登録サーバなどによってグループ情報が管理されていないことにより、二つの問題が生じうる。

【００２５】

第一の問題は、グループ情報の詐称である。図１１において、ネットワーク上に３つのグループＧ１、Ｇ２、Ｇ３が存在している。ここで、ユーザＡは自分がもとめるグループの条件αを作成し、Ｐ２Ｐネットワークに対してグループ情報の検索を行う（ステップ１１０１）。

【００２６】

次にＢ、ＦはＡからの検索をうけとり、自分の属するグループのグループ情報から、自分の属するグループがＡの指定した条件α適合するかを判定する。この例では、Ｇ２は条件αに適合しないため、Ｂ、Ｆはそれぞれ自分が知っているユーザに検索を転送する。そして、条件αに適合するグループのメンバ、この場合はＣ、Ｄは自分が保有するグループのグループ識別情報ＤＩ１および、グループ属性情報ＡＩ１を、Ａに通知する（ステップ１１０２）。この場合にはＡは自分の指定する条件に合うグループの存在を知り、参加することができる。

【００２７】

しかし、Ｐ２Ｐネットワークでは、図１２に示すように容易にグループ情報の詐称を行うことができる。ユーザＡは自分がもとめるグループの条件αを作成し

、Ｐ２Ｐネットワークに対して検索を行う（ステップ１２０１）。

【００２８】

この検索に対する応答として下記のような不正な応答が返される可能性がある。

【００２９】

（１）自分のグループに関するグループ属性情報を詐称する。

【００３０】

Ｂは、応答として自己のグループ識別情報ＤＩ２を使用し、それに対応するグループ属性情報として、自己のグループのグループ属性情報ＤＩ２ではなく、条件αに適合する。別のグループのグループ属性情報ＡＩ１を、使用してＡに送信する（ステップ１２０２）。この場合、Ａは自分の条件に合わないグループＧ２に参加してしまう可能性がある。

【００３１】

（２）他のグループのグループ識別情報を使用し、そのグループに関するグループ属性情報を詐称する。Ｅは、他のグループのグループのグループ識別情報ＤＩ１を使用し、条件αに適合するようグループ属性情報ＡＩ４を捏造して、Ａに送信する。（ステップ１２０３）ＡはグループＧ１に関して誤ったグループ属性情報を入手してしまい、かつ、グループＧ１は自己のグループについて誤ったグループ属性情報ＡＩ４を広められる危険性がある。また、エントリポイント情報を検索する際にも、同様に情報の詐称を行うことができる。

【００３２】

エントリポイント情報をＰ２Ｐネットワークの検索手段を使用して、検索する場合の処理の流れは図１１とほぼ同様である。検索するユーザは条件αとして、情報を入手したいグループのグループ識別情報を指定する。指定されたグループ識別情報によって特定されるグループに属しているユーザは、その検索に対する応答として、自身のエントリポイントの情報を応答として返す。

【００３３】

この際にも、グループ識別情報とエントリポイント情報の対応がサーバによって管理されていないために容易に、検索に対して不正な応答を返すことができる

。この場合には、下記の不正な応答が想定できる。

【００３４】

（３）他のグループのグループ識別情報を使用し、そのグループに関するエントリポイント情報を詐称する。ＥがグループＧ１のエントリポイント情報の検索に対して、Ｇ１のエントリポイント情報として、Ｂのエントリポイント情報を返すことができる。この場合、ＡはグループＧ１とは異なるＧ２参加してしまう可能性があり、グループＧ２のメンバＢはＡからの誤ったアクセスを処理しなければならない可能性がある。

【００３５】

上記のうち、（１）についてはサーバ・クライアントモデルについても起こりうる問題であるが、（２）（３）については、Ｐ２Ｐ環境においてより、生じやすい問題である。サーバによってグループ識別情報とグループ属性情報の対応、および、グループ識別情報とエントリポイント情報の対応が管理されていないため、悪意のあるユーザは、あるグループ識別情報によって識別されるグループのグループ属性情報やエントリポイント情報を改竄、捏造して検索として応答することが容易にできる。

【００３６】

このとき、応答を受け取ったユーザは、その対応が正しいものかを判断する方法が現在のＰ２Ｐネットワークによる情報検索では与えられていない。これは、従来のＰ２Ｐネットワークにおける検索手段では、検索者の検索に対し、任意の応答者が応答を返すことができることに原因がある。

【００３７】

第二の問題点は、グループに関する一意性である。グループが登録サーバによって一元的に管理されている場合、二つのグループを識別するための識別子はサーバによって容易に生成することができる。ユーザはこの識別子をグループ識別情報として使用することで、自分が情報を入手したいグループを一意に特定することができる。

【００３８】

しかし、Ｐ２Ｐネットワークにおいて、誰もが自由にグループを生成する場合

、各グループを一意に識別するための識別子を生成することは容易ではない。ユーザＡがグループを生成し、そのグループに識別子Ｇ１を与える。その後、ユーザＢもグループを生成し、そのグループの識別子としてＧ１を与えたとする。この時、別のユーザＣはＧ１という識別子によって、ユーザＡの生成したグループと、ユーザＢの生成したグループを識別することが出来ない。特に、ユーザＢが故意にユーザＡと同じグループの識別子を利用する事態が想定されるため、単に識別子の生成方法だけでは、この第二の課題を解決することはできない。故に、Ｐ２Ｐネットワークでグループを運用する際に、グループ識別情報として何を用いるべきかは大きな課題の一つである。

【００３９】

上記の第一、第二の課題を解決するために、グループやユーザに関する情報はサーバを使用することによって管理し、実際のデータ転送などをＰ２Ｐで行うといったアプローチを用いることもできる。この手法はＨｙｂｒｉｄ型Ｐ２Ｐと呼ばれ、前記サーバークライアントモデルの課題（３）および（４）を改善することができ、グループに関する情報の詐称を防ぐことができ、グループの一意性を確保することも容易にする。

【００４０】

しかし、サーバを導入することによって前記サーバークライアントモデルの課題（１）、（２）、（５）の問題点を解決できなくなる。

【００４１】

【非特許文献１】

小柳恵一編著、「Ｐ２Ｐ　インターネットの新世紀」、オーム社、２００２年5月１日

【００４２】

【発明が解決しようとする課題】

以上述べたように、サーバークライアントモデルの問題点を解決するためのＰ２Ｐネットワークにおいてグループでの情報共有を行う場合、

（１）グループ情報を管理するサーバを使用しない場合、情報を容易に改竄することができるため、検索に対する応答に信頼性がなくなるといった問題点があり

、（２）グループを一意に指定する識別子の生成が容易ではないといった問題点がある。また、（３）グループ情報を管理するサーバを使用する方法では運用コスト、信頼性といった問題点がある。

【００４３】

本発明は、上記問題点に鑑み、グループでの情報共有にサーバの運用を必要とせず、かつグループに関する情報を改竄することができず、かつグループの一意性を判断することができるグループ検索方法を提供することを目的とする。

【００４４】

【課題を解決するための手段】

本発明は、以上述べた課題を解決するため、以下のような構成をとるグループ情報入手方法、エントリポイント情報入手方法からなるグループ検索方法を提供する。

【００４５】

グループ検索方法の一実施形態は、ネットワーク上に存在するグループに参加するために必要な情報を含むグループ情報を入手するグループ情報入手ステップと、入手したグループ情報に対応するグループのエントリポイントを入手するエントリポイント情報入手ステップと、を実行することを特徴とする。

【００４６】

グループ情報入手方法の一実施形態は検索者がグループを検索するためのグループ検索メッセージを生成し、問い合わせを行うグループ情報検索ステップと、グループ検索メッセージを受け取った応答者が、グループ公開鍵を含むグループ情報を検索者に送信するためのグループ情報応答メッセージを生成し、応答を行うグループ情報応答ステップと、を実行することを特徴とする。

【００４７】

また、グループ情報入手方法の一実施形態は、前記グループ情報応答ステップにおいて、グループ管理者が保持するグループ秘密鍵に基づいてグループ情報応答メッセージを生成することを特徴とする。

【００４８】

また、グループ情報入手方法の一実施形態は、前記グループ情報応答ステップ

において、グループ管理者からグループ参加証発行許可証の発行をうけた発行者が、グループ参加証発行許可証に含まれる公開鍵に対応する秘密鍵に基づいてグループ情報応答メッセージを生成することを特徴とする。

【００４９】

エントリポイント情報入手方法の一実施形態は検索者がグループ公開鍵を含むグループ情報に基づいてエントリポイント検索メッセージを生成し、問い合わせを行うエントリポイント検索ステップと、前記エントリポイント検索メッセージを受信した応答者が受信したエントリポイント検索メッセージに対応するエントリポイント検索応答メッセージを生成し、応答を行うエントリポイント検索応答ステップと、を行うことを特徴とする。

【００５０】

また、エントリポイント入手方法の一実施形態は、前記エントリポイント検索応答ステップにおいて、エントリポイント検索メッセージの受信者が、エントリポイント検索メッセージに含まれるグループ公開鍵と応答者が保有するグループ公開鍵の比較によって、検索者の要求しているグループと応答者が所属しているグループの一意性を確認することを特徴とする。

【００５１】

また、エントリポイント入手方法の一実施形態は、前記エントリポイント検索応答ステップにおいて、エントリポイント検索メッセージの受信者が、エントリポイント検索メッセージに含まれるグループ公開鍵と応答者が保有するグループ公開鍵の比較だけでなく、検索メッセージに含まれるグループ公開鍵が、応答者が保有するグループ公開鍵更新履歴との比較によって、検索者の要求しているグループと応答者が所属しているグループの一意性を確認することを特徴とする。

【００５２】

また、エントリポイント入手方法の一実施形態は、前記エントリポイント検索応答ステップにおいて、グループの一意性が確認でき、かつエントリポイント検索メッセージに含まれるグループ公開鍵が、応答者の保有する最新のグループ公開鍵でない場合に、最新のグループ公開鍵を通知することを特徴とする。

【００５３】

また、エントリポイント入手方法の一実施形態は、前記エントリポイント検索応答ステップにおいて、応答者がグループ公開鍵、グループ参加証に基づいてエントリポイント検索応答メッセージを生成することを特徴とする。

【００５４】

【発明の実施の形態】

まず、本発明の実施形態の構成について概要を説明する。本発明はネットワークで互いに接続された複数の機器間の通信方法に関するものである。本発明はイーサネット（Ｒ）、アナログまたはデジタルの公衆回線または専用回線を用いたネットワーク、ＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅ）、無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などの物理的なネットワークを想定しているが、これらに制限されるものではない。また、インターネットではネットワークの下位プロトコルとしてＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）が広く使用されており本発明もその使用を想定しているが、これに制限されるものでもない。

【００５５】

前記機器のそれぞれに前記物理的なネットワークに対応した通信インタフェースが備わっており、前記通信インタフェースを制御して通信を行うためのプログラムを前記機器内のＣＰＵが実行することにより通信処理が行われる。

【００５６】

前記プログラムは前記機器のＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に記録されている場合、あるいは前記機器のハードディスクやリムーバブルディスクなど不揮発記憶装置に格納されていてそこから必要に応じて前記機器のＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）に読み込まれて実行される場合、あるいはこれらを組み合わせて実行する場合などがある。

【００５７】

また前記機器には機器使用者の入力を受け付けるための入力手段も備わっている。入力手段としては通常キーボード、マウス、タブレットなどが用いられる。これらの構成についてはパーソナルコンピュータなどで一般的に知られているも

のであり、本発明の主眼ではないので詳細な説明は省略する。

【００５８】

なお、以下で用いる「ユーザ」という用語は、前記機器、前記機器で動作するプログラムおよび機器使用者を含む概念である。

【００５９】

本発明が想定しているネットワークにおいては、各ユーザは、必ずしも常時ネットワークに接続しているわけではなく、通信に必要な各ユーザのアドレス情報（ＩＰアドレス、ポート番号など）も固定ではなくネットワークに接続するたびに変化する可能性がある。

【００６０】

（実施の形態１）

本発明の第一の実施の形態について説明する。

【００６１】

まず、本実施の形態で用いている公開鍵暗号化方式の概要を説明する。公開鍵暗号化方式とは、次のような数学的性質を持つ二つの暗号鍵、「公開鍵」と「秘密鍵」を用いた暗号化方式である。

【００６２】

（１）公開鍵と秘密鍵は、一方から現実的な時間で他方を計算することが互いに不可能である。

【００６３】

（２）公開鍵で暗号化した情報は対応する秘密鍵でのみ復号可能であり、逆もまた成立する。

【００６４】

上記（１）の性質により、利用者は秘密鍵のみを秘密裡に保持しておけば、公開鍵を第三者に知られても問題ないので公開鍵を公開しておくことができる。従って、情報を秘密裡に送信したい送信者は、前もって受信者の公開鍵を入手しておき情報を受信者の公開鍵で暗号化したものを送信する。受信者は自分のみが持つ秘密鍵でそれを復号することができ、暗号化前の情報を得ることができる。第三者が暗号化された情報を傍受しても、受信者の秘密鍵でしか復号できないため

情報が漏洩することはない。以下では、暗号化対象の情報Ｍを鍵Ｋで暗号化したものをｅ（Ｍ，Ｋ）のように表記することとする。

【００６５】

また、公開鍵暗号化方式を用いて、情報そのものは暗号化しないが、情報が改ざんされていないことを証明するための電子「署名」を行うことも可能である。すなわち、署名対象の情報Ｍから所定のアルゴリズムｆで一意に導き出される派生情報Ｈ＝ｆ（Ｍ）を送信者の秘密鍵ＫＳで暗号化したＳｇｎ＝ｅ（Ｈ，ＫＳ）を署名情報として元の情報Ｍに付加して送信する。受信者は、ＭとＳｇｎを受信し、Ｓｇｎを送信者の公開鍵ＫＰで復号化してＨを得て、Ｈ＝ｆ（Ｍ）が成立することを確認することで情報Ｍが第三者によって改ざんされていないことを確認できる。

【００６６】

なぜならば、Ｍが第三者により改ざんされていればＨ＝ｆ（Ｍ）が成立せず、また送信者の秘密鍵ＫＳがなければ、送信者の公開鍵ＫＰで正常に復号できるＳｇｎの作成も不可能だからである。

【００６７】

公開鍵暗号化方式、およびこれを応用した署名方式は、インターネットでセキュリティを要する通信に広く用いられている。以下では、あるユーザＡの公開鍵、秘密鍵をそれぞれＫＡ＿Ｐ、ＫＡ＿Ｓのように表記する。

【００６８】

本明細書においてグループは、次のように定義する。

【００６９】

（１）グループは一名以上のネットワーク参加者からなる

（２）一ユーザは複数のグループに属することが可能である

（３）グループにはグループ固有の共有情報がある

（４）同じグループに属することを互いに認証されたメンバ間では、そのグループの共有情報の送受信を行うことができる。グループを構成するメンバは、友人、家族、同じ趣味の持ち主、住所が近い者、の集合などが考えられる。

【００７０】

本実施の形態においては、グループを構成するメンバをグループ参加証を発行する権限をもつ管理者および一般ユーザに分類する。一般ユーザにグループ参加証を発行できるのは管理者のみであり、ユーザはグループ参加証を管理者に発行してもらうことでグループへの参加が可能となる。

【００７１】

Ｐ２Ｐネットワーク上でこのようなグループを発見し、グループのメンバにアクセスするためには以下に示すような処理が必要になる。

【００７２】

（１）グループの生成

（２）グループの告知

（３）グループ情報の取得

（４）エントリポイント情報の取得

（５）グループへの新規加入依頼

（６）グループメンバ間の認証

（７）グループメンバ間の情報共有

（８）グループ参加証の更新

（９）グループメンバの削除

（１０）グループ管理者の追加

（１１）グループ公開鍵の更新

以下、各処理について説明する。

【００７３】

１．グループの生成

情報共有のためにグループを作成したいユーザＡは、そのグループ用の公開鍵ＫＧ＿Ｐおよび秘密鍵ＫＧ＿Ｓのペアを作成する。これらはＡが指定した情報（パスフレーズ）を元に生成されたものであってもよいし、プログラムまたは装置が生成した乱数などの情報を元に生成されたものであってもよい。

【００７４】

２．グループの告知

生成したグループ公開鍵ＫＧ＿Ｐは、そのグループを特定するグループ識別情

報、例えば望ましくは他のグループと重複しないグループＩＤなどと共に何らかの方法でグループ情報として告知される。この告知方法としては、

（１）従来の技術の説明に用いた図１０にて例示したようなＰ２Ｐネットワークの全てあるいは一部のユーザを宛て先としてＡがグループ情報を発信し、そのグループ情報が図１５の検索情報の流れのようにユーザからユーザへと順次転送され、最終的に宛て先とされたユーザが受信することで実現してもよいし、

（２）物理的にＡと同じローカルエリアネットワーク（ＬＡＮ）または仮想プライベートネットワーク（ＶＰＮ）に属している他のユーザ宛てにグループ情報をブロードキャストすることで実現してもよいし、あるいは、

（３）Ａが電子メール、郵便等を含む、Ｐ２Ｐネットワークを介した転送以外の何らかの方法で他のユーザに対して少なくともグループ公開鍵ＫＧ＿Ｐを直接送信することで実現してもよいし、

さらには、

（４）グループ情報のリストを保持し検索の用途に供するグループ情報インデックスサーバを運営し、前記グループ情報をこのグループ情報インデックスサーバに登録することによって実現してもよいし、

（５）これらを複数組み合わせて実現することも可能である。

【００７５】

なお、前記グループ情報には、そのグループ名、グループの生成者を特定する情報、成り立ち、目的、参加条件等、当該グループの内容を説明する情報と共に告知されていても構わないし、グループ公開鍵ＫＧ＿Ｐのみをグループ情報として告知しても構わない。

【００７６】

３．グループ情報の取得

Ｐ２Ｐネットワークに参加しているユーザＸは、次のいずれかの方法でグループを発見し、グループを特定するグループ識別情報を取得する。本実施の形態では、グループ識別情報には、少なくともグループ公開鍵ＫＧ＿Ｐが含まれる。

【００７７】

（１）Ｘが保持している、過去に告知され受信したグループ情報（グループを

生成したＡから直接受け取ったグループ情報を含む）から、グループを特定するグループ識別情報あるいはグループを説明するグループ属性情報に基づき所望のグループを発見する。

【００７８】

（２）図１０に例示したようなＰ２Ｐネットワークの情報検索の仕組みを用いて他のユーザに対してグループ識別情報あるいはグループ属性情報の一部または全部をキーとして検索し、該当するグループ情報を保持しているユーザからグループ情報を入手する。

【００７９】

この際に、前述したグループ情報の詐称が問題になるが、この問題を解決するための方法の詳細は後述する。

【００８０】

（３）前記グループ情報インデックスサーバが運用されている場合には、このグループ情報インデックスサーバに対してグループ識別情報あるいはグループ属性情報の一部または全部をキーとして検索し、所望のグループのグループ情報を入手する。

【００８１】

（４）グループを生成したＡがＸにとって既知の場合は、グループ情報をＡから何らかの手段で直接入手する。

【００８２】

４．エントリポイント情報の取得

グループへの参加を行う際には、グループ管理者もしくは、グループメンバを特定し、そのエントリポイント情報を入手する必要がある。グループ管理者とは、グループメンバの追加削除の権限を持つユーザであり、より具体的にはグループ秘密鍵ＫＧ＿Ｓを保持するユーザである。あるグループへ新規加入したいユーザＸは、５．で説明するようにグループ管理者Ａと直接通信する必要があり、そのために必要なグループ管理者Ａのエントリポイント情報を取得する必要がある。

【００８３】

また、既にグループメンバとなっている場合でも、他のグループメンバと通信するために他のグループメンバのエントリポイント情報を取得する必要がある。それは例えば次のいずれかの方法で行われる。

【００８４】

（１）Ｘは図１０に例示したようなＰ２Ｐネットワークの情報検索の仕組みを用いてグループ識別情報の一部または全部をキーとして検索を行い、この検索要求を受けた該当するグループの管理者やメンバがこれに応答し、自分のアドレス情報をＸに対して通知する。

【００８５】

このときに前述したエントリポイント情報の詐称の問題が生じるが、これを解決するための方法についての詳細は、後述する。

【００８６】

（２）現在オンライン状態である全ユーザ、あるいは少なくとも一つのグループの管理者である全ユーザの、少なくともアドレス情報および当該ユーザが管理者であるグループのグループを特定する情報を収集して検索の用途に供するピア情報サーバが運営されている場合、Ｘはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果として管理者や、グループメンバのアドレス情報を入手する。

【００８７】

（３）グループ管理者ＡがＸにとって既知であり、かつグループ管理者Ａが常にオンラインであってアドレス情報が変化しないことも既知である場合、そのアドレス情報を用いる。

【００８８】

５．グループへの新規加入依頼

あるグループへ新規加入したいユーザＸは、前記４．で特定したアドレス情報を用いてグループ管理者Ａと通信を行い、６．で必要となるグループ参加証の発行を依頼する。

【００８９】

６．グループメンバ間の認証

前記５．で入手したグループ参加証を持つグループメンバ間では、互いに同じグループに属していることを認証することが可能になる。

【００９０】

７．グループメンバ間の情報共有

前記６．で互いに同じグループに属していると認証された複数のグループメンバ間、例えばＸとＹの間ではグループの共有情報の相互の転送が可能になる。これは、例えば次のようなステップを順に実行することにより行われる。

【００９１】

（７－１）通信に用いる暗号鍵の設定

前記６．で互いに同じグループに属していることを認証した後、暗号鍵Ｋ＿ＸＹを一方、例えばＸ、が作成して、Ｘの秘密鍵およびＹの公開鍵でこの暗号鍵を暗号化してＹに送付する。Ｙはこれを自分の秘密鍵およびＸの公開鍵を用いて復号可能であり、またＹ以外はこれを復号することができない。これにより、安全にＫ＿ＸＹをＸからＹに通知する。

【００９２】

（７－２）情報転送の暗号化

以降のＸとＹの間の情報転送は、Ｋ＿ＹＸで暗号化して行う。第三者はＫ＿ＸＹを知ることができないので、ＸＹ間の通信を傍受してもその内容を復号することはできず、また、ＸまたはＹに成りすまして偽の情報をＹまたはＸに転送することも不可能となり、ＸとＹは安全に情報転送を行うことができる。これにより、グループメンバ相互間での安全なグループ情報の共有が可能となる。

【００９３】

なお、３名以上のメンバがお互いに認証された状態である場合、このメンバ間の情報転送に用いる暗号鍵には次のような選択肢がある。

【００９４】

（１）異なる二者間の通信には異なる暗号鍵を用いる。

【００９５】

例えば、ＡとＢとＣが互いに認証されている場合、ＡとＢの間の通信には暗号鍵Ｋ＿ＡＢを、ＢＣ間はＫ＿ＢＣ、ＣＡ間はＫ＿ＣＡを用いる方法である。

【００９６】

（２）互いに認証された複数メンバ間で共通の暗号鍵を用いる。

【００９７】

例えば、ＡとＢが互いに認証されていて暗号鍵Ｋ＿ＡＢを用いて通信している状態でＣが新たにＡまたはＢとの認証処理を行って認証された場合、ＡまたはＢからＣへＣの公開鍵を用いて安全にＫ＿ＡＢを送付し、以降はＡ、Ｂ、Ｃのいずれの二者間でも暗号鍵Ｋ＿ＡＢを用いる方法である。

【００９８】

８．グループ参加証の更新

前記５．で発行されるグループ参加証に有効期限情報が含まれている場合には、当該有効期限以降グループへの参加（グループメンバ間の認証）が不可能になるため、ユーザはグループ参加証の更新が必要となる。

【００９９】

９．グループメンバの削除

上記で述べてきた方法では、グループ参加証を持つユーザは、そのグループ参加証の有効期限まではグループへの参加が可能であるが、何らかの理由により、その有効期限以前にそのユーザをグループメンバから除外したい（そのユーザをグループメンバとして認証できないようにしたい）場合は、例えば次のような処理を実行することで可能となる。

【０１００】

（９－１）グループ参加証の消去

除外対象メンバが保持しているグループ参加証を消去すれば、当該メンバはその後は前記６．で述べたグループメンバ間の認証が行えなくなる。そのためには次のような処理を実行する必要がある。

【０１０１】

（９－１－１）グループ参加証の消去指示

グループ管理者がメンバを除外することを指定することを指示する参加証消去指示ステップを実行する。

【０１０２】

（９－１－２）グループ参加証の消去

上記参加証消去指示を受けた当該メンバは、自分が保持しているグループ参加証を消去する。これは機器の使用者が手動で消去する方法でも良いが、この場合は指示を無視して故意に消去しない場合も考えられるので、上記参加証消去指示を受けた機器あるいはプログラムが強制的に消去する方法でもよい。

【０１０３】

しかし、この方法でグループ参加証を消去するには、グループ管理者と除外対象メンバが同時にオンラインである必要があり、必ずしも除外対象メンバのグループ参加証が消去できるとは限らない。この問題を解決するには次のような方法が考えられる。

【０１０４】

（９－２－１）失効者情報の作成

グループメンバの一人（グループ管理者含む）が、除外されたメンバを特定する情報、例えば当該メンバの公開鍵、を含む失効者情報を作成する。

【０１０５】

（９－２－２）失効者リストの共有

前記６．のグループメンバ間の認証の際には、自分が保持する失効者情報のリストと認証相手が持つ失効者情報のリストを比較し、一方が保持しない失効者情報が存在する場合は互いに他方の失効者リストに追加することで、失効者情報のリストを全グループメンバで共有するようにする。

【０１０６】

（９－２－３）失効者の除外

前記６．のグループメンバ間の認証の際に、認証相手が自分の保持する失効者リストに含まれているかどうかを確認し、含まれている場合は相手をグループメンバであると認証しない。例えばユーザの公開鍵を失効者情報として用いる場合は、認証相手の公開鍵がリストに含まれる失効者情報のいずれかと一致すれば、この相手の認証を拒否する。

【０１０７】

（９－２－４）失効者の参加資格更新の拒否

前記８．においてグループ参加証の更新を行う際に、参加証の更新を依頼したユーザがリストに含まれる失効者情報のいずれかと一致するかどうかを確認し、一致するものがある場合は参加証の更新を拒否する。

【０１０８】

なお、失効者情報にその消去期限を含めておいて、消去期限を越えた失効者情報を削除することが可能である。例えば、グループ参加証の有効期限より少し後の時点を消去期限として付与しておけば、不要となった失効者情報を順次削除することができ、失効者情報のリストが無限に増大することを防ぐことができる。

【０１０９】

また、失効者情報の作成はグループ管理者のみが行い、グループ管理者がグループ秘密鍵ＫＧ＿Ｓを用いて暗号化した状態で共有することとしてもよい。グループメンバは公開されているグループ公開鍵ＫＧ＿Ｐを用いて失効者情報を復号することが可能であり、この失効者情報が不正に改ざんされていないことの確認が可能となる。これにより、悪意を持つユーザにより作成された不正な失効者情報が共有されることを防ぐことができる。

【０１１０】

１０．グループ管理者の追加

前記５．で述べたグループへの新規加入は、グループ管理者がオンラインである場合にしか行えない。グループ生成直後はグループを生成したユーザ一人のみがグループ管理者であるが、グループへの新規加入の機会を増やすために、グループ管理者を増やすことが可能である。これは、グループ秘密鍵ＫＧ＿Ｓを何らかの安全な手段、すなわち暗号化通信または郵送などの手段によってグループ管理者から別のユーザに転送することによって実現することができる。

【０１１１】

１１．グループ公開鍵の更新

何らかの事故によりグループ秘密鍵ＫＧ＿Ｓがグループ管理者以外のユーザに漏洩した場合、グループ秘密鍵を入手したユーザは不正にグループ参加証または失効者リストを発行することが可能となり、かつグループメンバには本来のグループ管理者が発行したグループ参加証と不正に発行されたグループ参加証を判別

することはできない。このような場合には、グループ公開鍵・秘密鍵のペアを更新する以外に不正を防ぐ方法はない。

【０１１２】

また、前記１０．で追加されたグループ管理者のいずれかからユーザ追加削除の権限を剥奪したい場合も、グループ公開鍵・秘密鍵のペアを更新する以外の方法はない。

【０１１３】

一方、グループ管理者がグループ公開鍵・秘密鍵をそれぞれＫＧ＿Ｐ’、ＫＧ＿Ｓ’に更新したとしても、従来のグループ公開鍵ＫＧ＿Ｐとそれに基づいて作成されたグループ参加証を持つグループメンバ同士では前記６．のグループ認証は互いに可能なままなので、グループメンバは常に最新のグループ公開鍵を保持しておく必要があると同時に、最新のグループ公開鍵に対応したグループ参加証を入手する必要がある。

【０１１４】

最新のグループ公開鍵の保持は、例えば次のいずれかのような方法により可能である。

【０１１５】

（１）グループ管理者がグループ公開鍵・秘密鍵を更新した時点で、図１０に例示したようなＰ２Ｐネットワークを介してネットワーク参加者全員に新しいグループ公開鍵を送付する。対応するグループのメンバは、この新しいグループ公開鍵で自分が保持しているグループ公開鍵を置き換える。

【０１１６】

（２）前記２．で告知されるグループ情報に、グループ公開鍵の更新時刻に関する情報も含めておき、前記各グループメンバはグループ公開鍵に加えてこのグループ公開鍵の更新時刻に関する情報も保持しておく。そして、前記６．のグループ認証時には双方が持つグループ公開鍵とその更新時刻の比較を行い、新しい方のグループ公開鍵で古いほうのグループ公開鍵を置き換える。

【０１１７】

（３）前記２．の（４）におけるグループ情報インデックスサーバを運営して

いる場合には、グループ情報に（１）同様グループ公開鍵の更新時刻に関する情報も含めておき、グループメンバはオンラインになった時、一定時間おき、あるいは前記６．のグループ認証を行う直前、などのタイミングで前記グループ情報インデックスサーバにアクセスして当該グループの最新のグループ公開鍵を入手する。

【０１１８】

最新のグループ公開鍵に対応したグループ参加証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼（前記８．）を実行すればよい。

【０１１９】

（４）前記３．の（２）もしくは、前記４．の（１）のように、Ｐ２Ｐネットワークの情報検索の仕組みを用いてグループ情報やエントリポイント情報の検索が行われた際の応答として最新のグループ公開鍵を通知する。

【０１２０】

この場合、検索者は検索のためのメッセージに、グループ公開鍵を含めておく。グループのメンバはグループ公開鍵の履歴を保存しておき、受け取ったメッセージに含まれるグループ公開鍵が、自身のグループ公開鍵の履歴に含まれる場合に、検索の応答として、最新のグループ公開鍵を送信する。エントリポイント情報の検索に対して、最新のグループ公開鍵を通知する方法の詳細については後述する。

【０１２１】

次に、前記３．で概要を述べたＰ２Ｐネットワークでの情報検索の仕組みを用いたグループ情報の取得の処理の流れについて図１と図２を参照して順を追って詳細に説明する。図１はグループの検索を行う検索者Ｘとグループ管理者Ａでそれぞれ実行される処理の流れを図示したものである。図２はグループの検索が終了したあと、検索者Ｘが保持している情報をあらわしている。

【０１２２】

［ステップ１０１］

事前に、グループ管理者Ａはグループの公開鍵ＫＧ＿Ｐ・秘密鍵ＫＧ＿Ｓのペ

アを作成する。また、ＫＧ＿Ｐを含むグループ情報ＩＧを生成する。

【０１２３】

ＫＧ＿ＰおよびＩＧについては公開しておいても構わない。（前記１．および前記２．を参照）。

【０１２４】

［ステップ１０２］

検索者Ｘは検索したいグループの条件ＣＧを作成する。このとき指定される条件はグループのカテゴリなどが考えられるが特に規定されるものではない。また、条件記述の形式も特に限定されるものではない。

【０１２５】

［ステップ１０３］

Ｘは作成したＣＧを含むグループ検索メッセージＭＧ＿Ｑを生成して送信する。この時の送信方法は、ブロードキャスト、マルチキャスト、Ｐ２Ｐネットワークによるメッセージ伝播などで送信されるが、送信方法は特に限定されるものではない。

【０１２６】

［ステップ１０４］

Ａはグループ検索メッセージＭＧ＿Ｑを受け取り、ＭＧ＿Ｑに含まれるＣＧと自分が管理するグループのグループ情報ＩＧとを比較し、自分が管理するグループがＣＧで指定される条件に適合するかを判定する。この判定は管理者が自分で判断しても良いし、プログラムなどで自動的に判定しても良い。ＣＧとＩＧが適合しない場合は、ＡはＭＧ＿Ｑを破棄して処理を終了する、またはＭＧ＿Ｑを別のユーザに送信して処理を終了する。

【０１２７】

［ステップ１０５］

ＡはＫＧ＿Ｐを含むＩＧからグループ情報応答メッセージＭＧ＿Ａを作成する。Ａはグループ秘密鍵ＫＧ＿Ｓを使用してＭＧ＿Ａに署名を施した後、Ｘに向けて送信する。

【０１２８】

［ステップ１０６］

ＸはＡからＭＧ＿Ａを受け取ると、ＭＧ＿Ａに含まれるＫＧ＿Ｐを入手する。

【０１２９】

［ステップ１０７］

ＸはＫＧ＿Ｐを使用して、ＭＧ＿Ａの署名の有効性を確認する。署名の有効性が確認されない場合は、ＭＧ＿Ａは第三者によって改竄されている可能性があるために、ＸはＭＧ＿Ａを破棄して処理を終了する。

【０１３０】

［ステップ１０８］

ＸはＭＧ＿ＡからＩＧを入手する。

【０１３１】

［ステップ１０９］

ＸはＩＧとＣＧを比較し、両者が適合するかを判定する。

【０１３２】

適合しないと判定した場合、ＸはＭＧ＿Ａを破棄して、処理を終了する。

【０１３３】

［ステップ１１０］

ＸはＡから受信したＭＧ＿Ａに含まれるＩＧを保存する。また、必ずしも管理者がメッセージを生成するのではなく、以前に管理者が生成した応答メッセージを別のユーザがキャッシュしておき応答に使用する実施形態も考えられる。

【０１３４】

上記の方法を用いることによって、検索者Ｘは応答として入手できたグループの情報がグループ公開鍵ＫＧ＿Ｐを有するグループの管理者によって作成されたものであることが確認できる。

【０１３５】

つまり、グループを一意に特定する識別子として、グループ公開鍵を使用し、グループ情報にグループ秘密鍵による署名を付加することによって、グループの管理者以外が、そのグループに関する情報を詐称することを防止することができる。

【０１３６】

また、仮に他のグループＧ２の管理者が自己のグループの識別子として、グループＧ１のグループ公開鍵を使用した場合にも、現状では十分な長さをもつ公開鍵から秘密鍵を計算することは事実上困難であるため、Ｇ１のグループ秘密鍵までも詐称することができない。

【０１３７】

この方法によって、グループ情報の詐称、グループを一意性の確認の課題を解消することができる。

【０１３８】

ただ、グループ公開鍵を安全性の確保のために時折更新する場合には、グループの一意性を確認するための識別子として単一のグループ公開鍵を使用することはできない。この場合には、後述するように、グループの公開鍵の履歴を使用してグループの一意性を確保する必要がある。

【０１３９】

次に、前記４．で概要を説明した、Ｐ２Ｐネットワークの情報検索の仕組みを用いたグループのエントリポイント検索について図３、図４を用いて詳細に説明する。図３は検索者Ｘとグループ参加者Ｙでそれぞれ実行される処理の流れを図示したものである。図４はエントリポイント検索が終了したあと、検索者Ｘが保持している情報をあらわしている。

【０１４０】

［ステップ３０１］

検索者Ｘはエントリポイントを入手したいグループのグループ公開鍵ＫＧ＿Ｐを含むエントリポイント検索メッセージＭＥ＿Ｑを生成して、送信する。このときの送信方法は、ブロードキャスト、マルチキャスト、ユニキャスト、Ｐ２Ｐネットワークによるメッセージ伝播など様々な方法が考えられるが、ここでは特定の送信方法に限定されない。

【０１４１】

［ステップ３０２］

ＭＥ＿Ｑを受信した参加者Ｙは、ＭＥ＿Ｑに含まれるＫＧ＿Ｐを入手し、Ｙが

参加しているグループの公開鍵ＫＧ＿Ｐ’と比較する。

【０１４２】

［ステップ３０３］

二つの公開鍵が一致しない場合にはＹはＭＥ＿Ｑを破棄して処理を終了するか、もしくは、ＭＥ＿Ｑを別のユーザに送信して処理を終了する。

【０１４３】

［ステップ３０４］

Ｙは自分のグループ参加証Ｃ＿Ｘおよび、自身のエントリポイント情報ＥＹを含むエントリポイント検索応答メッセージＭＥ＿Ａを作成する。ＹはＭＥ＿Ａに対して自身の秘密鍵ＫＹ＿Ｓで署名を行い、署名されたＭＥ＿ＡをＸに送信する。

【０１４４】

［ステップ３０５］

Ｘは受信したＭＥ＿ＡからＣ＿Ｙを取得する。

【０１４５】

［ステップ３０６］

ＸはＫＧ＿Ｐを使用してＣ＿Ｙの有効性を確認する。簡単には（１）ＫＧ＿Ｐで正常に復号化できる、あるいは署名を確認できるか。（２）有効期限は切れていないかの二点によってＣ＿Ｙの有効性は確認できる。Ｃ＿Ｙの有効性が確認できない場合、ＸはＭＥ＿Ａを破棄して処理を終了する。

【０１４６】

［ステップ３０７］

Ｃ＿ＹからＹの公開鍵ＫＹ＿Ｐを取得する。ＫＹ＿Ｐを使用して、ＭＥ＿Ａの署名を確認する。

【０１４７】

［ステップ３０８］

ＭＥ＿Ａの署名の正当性が確認できない場合、ＭＥ＿Ａは第三者によって改竄された可能性があるため、ＸはＭＥ＿Ａを破棄して処理を終了する。

【０１４８】

［ステップ３０９］

ＸはＹをＫＧ＿Ｐによって特定されるグループのメンバであると認定し、ＥＹをグループのエントリポイントとして記憶する。

【０１４９】

上記の方法のように、グループを一意に識別する情報としてグループ公開鍵を使用し、応答にグループ公開鍵で指定されるグループのメンバであることを証明する情報を含めることによって、グループメンバ以外のユーザがエントリポイント情報を詐称することを防ぐことができる。

【０１５０】

次に、前記１１．の（４）で概要を説明した、グループ公開鍵の更新方法について図５、図６を参照して順をおって詳細に説明する。図５はエントリポイント検索者Ｘとそのグループ公開鍵に対応するグループの参加者Ｙでそれぞれ実行される処理の流れを図示したものである。図６はグループ公開鍵の通知を受けたあと、検索者Ｘが保持している情報をあらわしている。

【０１５１】

［ステップ５０１］

検索者Ｘはエントリポイントを入手したいグループのグループ公開鍵ＫＧ＿Ｐを含むエントリポイント検索メッセージＭＥ＿Ｑを生成して、送信する。このときの送信方法は、ブロードキャスト、マルチキャスト、ユニキャスト、Ｐ２Ｐネットワークによるメッセージ伝播などが用いられるが、ここでは特定の送信方法に限定しない。

【０１５２】

［ステップ５０２］

ＭＥ＿Ｑを受信した参加者Ｙは、ＭＥ＿Ｑに含まれるＫＧ＿Ｐを入手する。

【０１５３】

［ステップ５０３］

Ｙは自分が参加しているグループの公開鍵ＫＧ＿Ｐ’とＫＧ＿Ｐを比較する。このとき、二つの公開鍵が一致する場合には、前記図３のステップ３０４以降の処理を実行する。

【０１５４】

［ステップ５０４］

ＹはＫＧ＿Ｐが、自分が属しているグループ公開鍵の履歴ＨＧに含まれているかを判定する。

【０１５５】

［ステップ５０５］

ＫＧ＿ＰがＨＧに含まれていない場合にはＹはＭＥ＿Ｑを破棄して処理を終了する、もしくは、ＭＥ＿Ｑを別のユーザに送信して処理を終了する。

【０１５６】

［ステップ５０６］

ＹはＨＧと共に、履歴に対応するグループ公開鍵変更メッセージを所有している。グループ公開鍵がＫＧ＿Ｐ（Ｉ）からＫＧ＿Ｐ（Ｉ＋１）に変更される場合には、グループ管理者から、グループ公開鍵変更メッセージＭＣ＿Ｋ（Ｉ）が、グループメンバに通知される。ＭＣ＿Ｋ（Ｉ）は、ＫＧ＿Ｐ（Ｉ＋１）を含み、それに対してＫＧ＿Ｐ（Ｉ）、ＫＧ＿Ｐ（Ｉ＋１）で署名されており、以前のグループ秘密鍵、および最新のグループ秘密鍵を所有する管理者が発行したことが確認できる。

【０１５７】

ＫＧ＿ＰがグループのＩ番目の鍵、ＫＧ＿Ｐ’がグループのＩ＋Ｊ番目の鍵であった場合、ＹはＭＣ＿Ｋ（Ｉ＋１）からＭＣ＿Ｋ（Ｉ＋Ｊ）までＪ個のグループ公開鍵変更メッセージを含むグループ公開鍵通知メッセージＭＵ＿Ｋを作成し、Ｘに送信する。

【０１５８】

［ステップ５０７］

Ｘは受信したＭＵ＿Ｋを受信し、Ｋ＝１として以降の処理を実行する。

【０１５９】

［ステップ５０８］

Ｘは受信したＭＵ＿Ｋから、ＭＣ＿Ｋ（Ｉ＋Ｋ）を取得する。

【０１６０】

［ステップ５０９］

ＸはＫＧ＿Ｐ（Ｉ＋Ｋ－１）を使用して、ＭＣ＿Ｋ（Ｉ＋Ｋ）の署名を確認する。

【０１６１】

［ステップ５１０］

署名の正当性が確認されない場合は、ＭＵ＿Ｋを破棄して処理を終了する。

【０１６２】

［ステップ５１１］

証明の正当性が確認できた場合は、ＭＣ＿Ｋ（Ｉ＋Ｋ）から、ＫＧ＿Ｐ（Ｉ＋Ｋ）を取得する。

【０１６３】

［ステップ５１２］

ＫとＪが等しいかを判定する。ＫがＪと等しくない場合はステップ５１３の処理を、ＫとＪが等しい場合はステップ５１４の処理を実行する。

【０１６４】

［ステップ５１３］

Ｋ＝Ｋ＋１として、ステップ５０８以降の処理を繰り返す。

【０１６５】

［ステップ５１４］

ＫＧ＿Ｐ’＝ＫＧ＿Ｐ（Ｉ＋Ｊ）を最新のグループ公開鍵としてＫＧ＿Ｐと置き換える。

【０１６６】

上記の方法のように、グループ公開鍵の履歴によってグループの一意性を判定することによってグループ公開鍵のように更新される情報をグループの識別子として使用することが可能になる。

【０１６７】

また、上記の手法をとることで、古いグループの公開鍵しか所有していないユーザであっても最新のグループ公開鍵の通知を受けることができ、通知された最新のグループ公開鍵の正当性を以前のグループ公開鍵によって確認することがで

きる。

【０１６８】

上記に述べたように、グループに対して固有のグループ公開鍵を設定することで、グループの一意性の確認の問題、グループに対する情報の詐称の問題を解決することができる。

【０１６９】

（実施の形態２）

前述した第一の実施の形態では、グループを構成するメンバとしては管理者と一般ユーザだけとしているが、第一の実施の形態の１０．で述べたように、グループメンバの新規加入機会を増やすためには管理者を増やす、すなわちグループ秘密鍵を複製することが必要であるが、グループ秘密鍵が複数のユーザに保持されることで、漏洩する可能性が高くなるという課題がある。

【０１７０】

本実施の形態はこれを改善するものであり、グループを構成するメンバを唯一の管理者、グループ参加証発行許可証を保持し、グループ参加証を発行する権限を持つ発行者、および一般ユーザに分類する。発行者に権限を与えることができるのは管理者のみであり、一般ユーザにグループ参加証を発行できるのは管理者および発行者である。こうすることにより、管理者が複数の発行者を設けておけば、グループの秘密鍵を複製することなくユーザの新規加入機会を増やすことが可能となる。

【０１７１】

このようなグループを管理するには、以下に示すような処理が必要となる。

【０１７２】

（１）グループの生成

（２）グループの告知

（３）グループ発行者の追加

（４）グループ情報の取得

（５）エントリポイント情報の取得

（６）グループへの新規加入依頼

（７）グループメンバ間の認証

（８）グループメンバ間の情報共有

（９）グループ参加証の更新

（１０）グループ参加証発行許可証の更新

（１１）グループメンバの削除

（１２）グループ公開鍵の更新

以下、各処理について説明する。ただし、第一の実施の形態と同一のものについてはその旨記して説明を省略している。

【０１７３】

１．グループの生成

第一の実施の形態の１．グループの生成と同じであるので省略する。

【０１７４】

２．グループの告知

第一の実施の形態の２．グループの告知と同じであるので省略する。

【０１７５】

３．グループ発行者の追加

前記１．でグループを生成したユーザ（グループ管理者）は、グループ参加証発行許可証を発行することでグループメンバを追加する権限を持つユーザを必要人数追加することができる。すなわち、グループ参加証発行許可証を発行されたユーザは他のユーザに対してグループ参加証を発行することが可能となる。グループ管理者がグループ参加発行許可証を発行したユーザをグループ発行者と呼ぶ。

【０１７６】

４．グループの発見

Ｐ２Ｐネットワークに参加しているユーザＸは、次のいずれかの方法でグループを発見し、グループを特定するグループ識別情報を取得する。本実施の形態では、グループ識別情報には、少なくともグループ公開鍵ＫＧ＿Ｐが含まれる。

【０１７７】

（１）Ｘが保持している、過去に告知され受信したグループ情報（グループを

生成したＡから直接受け取ったグループ情報を含む）から、グループを特定するグループ識別情報あるいはグループを説明するグループ属性情報に基づき所望のグループを発見する。

【０１７８】

（２）図１０に例示したようなＰ２Ｐネットワークの情報検索の仕組みを用いて他のユーザに対してグループ識別情報あるいはグループ属性情報の一部または全部をキーとして検索し、該当するグループ情報を保持しているユーザからグループ情報を入手する。

【０１７９】

この際に、前述したグループ情報の詐称が問題になるが、この問題を解決するための方法の詳細は後述する。

【０１８０】

（３）前記グループ情報インデックスサーバが運用されている場合には、このグループ情報インデックスサーバに対してグループ識別情報あるいはグループ属性情報の一部または全部をキーとして検索し、所望のグループのグループ情報を入手する。

【０１８１】

（４）グループを生成したＡがＸにとって既知の場合は、グループ情報をＡから何らかの手段で直接入手する。

【０１８２】

５．エントリポイントの特定

グループへの参加を行う際には、グループ管理者、グループ発行者もしくは、グループメンバを特定し、そのエントリポイント情報を入手する必要がある。あるグループへ新規加入したいユーザＸは、５．で説明するようにグループ発行者Ｂと直接通信する必要があり、そのために必要なグループ発行者Ｂのエントリポイント情報を取得する必要がある。

【０１８３】

また、既にグループメンバとなっている場合でも、他のグループメンバと通信するために他のグループメンバのエントリポイント情報を取得する必要がある。

それは例えば次のいずれかの方法で行われる。

【０１８４】

（１）Ｘは図１０に例示したようなＰ２Ｐネットワークの情報検索の仕組みを用いてグループ識別情報の一部または全部をキーとして検索を行い、この検索要求を受けた該当するグループの発行者やメンバがこれに応答し、自分のアドレス情報をＸに対して通知する。このときに前述したエントリポイント情報の詐称の問題が生じるが、これを解決するための方法についての詳細は、後述する。

【０１８５】

（２）現在オンライン状態である全ユーザ、あるいは少なくとも一つのグループの管理者である全ユーザの、少なくともアドレス情報および当該ユーザが管理者であるグループのグループを特定する情報を収集して検索の用途に供するピア情報サーバが運営されている場合、Ｘはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果として管理者や、グループメンバのアドレス情報を入手する。

【０１８６】

（３）グループ発行者ＢがＸにとって既知であり、かつグループ発行者Ｂが常にオンラインであってアドレス情報が変化しないことも既知である場合、そのアドレス情報を用いる。

【０１８７】

６．グループへの新規加入依頼

グループへ新規加入したいユーザＸは、前記５．で特定したアドレス情報を用いてグループ発行者と通信を行い、７．で必要となるグループ参加証の発行を依頼する。

【０１８８】

７．グループメンバ間の認証

前記６．で入手したグループ参加証を持つグループメンバ間では、互いに同じグループに属していることを認証することが可能になる。

【０１８９】

８．グループメンバ間の情報共有

第一の実施の形態の前記７．と同じであるので省略する。

【０１９０】

９．グループ参加証の更新

前記６．で発行されるグループ参加証に有効期限情報が含まれている場合には、当該有効期限以降グループへの参加（グループメンバ間の認証）が不可能になるため、ユーザはグループ参加証の更新が必要となる。

【０１９１】

１０．グループ参加証発行許可証の更新

前記３．で発行されたグループ参加証発行許可証に有効期限情報が含まれている場合には、当該有効期限以降グループ参加証の発行が不可能になるため、発行者はグループ参加証発行許可証の更新が必要となる。

【０１９２】

１１．グループメンバの削除

第一の実施の形態同様、何らかの理由により、グループ参加証の有効期限以前に特定のメンバをグループメンバから除外したい場合がありえる。

【０１９３】

当該メンバのグループ参加証を消去する方法は、第一の実施の形態の前記９．における方法において「グループ管理者」を「グループ管理者またはグループ発行者」に置き換えた場合と同一であるので詳細な説明は省略する。

【０１９４】

第一の実施の形態同様、失効者情報を作成・共有する方法をとることも可能である。すなわち、例えば次のような処理を実行する。

【０１９５】

（１１－１）失効者情報の作成

グループメンバの一人（グループ管理者、グループ発行者含む）が、除外されたメンバを特定する情報、例えば当該メンバの公開鍵、を含む失効者情報を作成する。

【０１９６】

（１１－２）失効者リストの共有

前記７．のグループメンバ間の認証の際には、自分が保持する失効者情報のリストと認証相手が持つ失効者情報のリストを比較し、一方のリストに含まれない失効者情報が存在する場合は互いに他方のリストに追加することで、失効者情報のリストを全グループメンバで共有するようにする。

【０１９７】

（１１－３）失効者の除外

前記７．のグループメンバ間の認証の際に、認証相手が自分の保持する失効者情報のリストに含まれているかどうかを確認し、含まれている場合は相手をグループメンバであると認証しない。例えばユーザの公開鍵を失効者情報として用いる場合は、認証相手の公開鍵がリストに含まれる失効者情報のいずれかと一致すれば、この相手の認証を拒否する。

【０１９８】

（１１－４）失効者の参加資格更新の拒否

前記９．においてグループ参加証の更新を行う際に、参加証の更新を依頼したユーザがリストに含まれる失効者情報のいずれかと一致するかどうかを確認し、一致するものがある場合は参加証の更新を拒否する。

【０１９９】

なお、失効ユーザ情報にその消去期限を含めておいて、消去期限を越えた失効者情報を削除することが可能であるのは第一の実施の形態同様である。

【０２００】

また、第一の実施の形態同様、失効者情報の作成はグループ発行者のみが行い、グループ発行者が自分の秘密鍵を用いて暗号化した状態で共有することとしてもよい。グループメンバは失効者情報とそれを発行したグループ発行者の参加証発行許可証を同時に入手することにより、この参加証発行許可証に含まれるグループ発行者の公開鍵を用いて失効者情報を復号することが可能であり、この失効者情報が不正に改ざんされていないことの確認が可能となる。これにより、悪意を持つユーザにより作成された不正な失効者情報が共有されることを防ぐことができる。

【０２０１】

１２．グループ公開鍵の更新

何らかの事故によりグループ秘密鍵ＫＧ＿Ｓがグループ管理者以外のユーザに漏洩した場合、グループ秘密鍵を入手したユーザは不正にグループ参加証発行許可証を発行することが可能となり、ひいてはグループ参加証を不正に発行することが可能となる。このときグループメンバには不正なグループ参加証発行許可証やグループ参加証と正規のものを判別することはできない。このような場合には、グループ公開鍵・秘密鍵のペアを更新する以外に不正を防ぐ方法はない。

【０２０２】

一方、グループ管理者がグループ公開鍵・秘密鍵をそれぞれＫＧ＿Ｐ’、ＫＧ＿Ｓ’に更新したとしても、従来のグループ公開鍵ＫＧ＿Ｐとそれに基づいて作成されたグループ参加証発行許可証を持つグループメンバ同士では前記６．のグループ認証は互いに可能なままなので、グループメンバは常に最新のグループ公開鍵を保持しておく必要があると同時に、最新のグループ公開鍵に対応したグループ参加証を入手する必要がある。発行者はこれに加えて最新のグループ鍵に対応したグループ参加証発行許可証を入手する必要がある。

【０２０３】

最新のグループ公開鍵の保持は、第一の実施の形態同様、例えば次のいずれかのような方法により可能である。

【０２０４】

（１）グループ管理者がグループ公開鍵・秘密鍵を更新した時点で、図１５に例示したようなＰ２Ｐネットワークを介してネットワーク参加者全員に新しいグループ公開鍵を送付する。対応するグループのメンバは、この新しいグループ公開鍵で自分が保持しているグループ公開鍵を置き換える。

【０２０５】

（２）前記２．で告知されるグループ情報に、グループ公開鍵の更新時刻に関する情報も含めておき、前記各グループメンバはグループ公開鍵に加えてこのグループ公開鍵の更新時刻に関する情報も保持しておく。そして、前記６．のグループ認証時には双方が持つグループ公開鍵とその更新時刻の比較を行い、新しい方のグループ公開鍵で古いほうのグループ公開鍵を置き換える。

【０２０６】

（３）前記２．の（４）におけるグループ情報インデックスサーバを運営している場合には、グループ情報に（１）同様グループ公開鍵の更新時刻に関する情報も含めておき、グループメンバはオンラインになった時、一定時間おき、あるいは前記６．のグループ認証を行う直前、などのタイミングで前記グループ情報インデックスサーバにアクセスして当該グループの最新のグループ公開鍵を入手する。

【０２０７】

最新のグループ公開鍵に対応したグループ参加証発行許可証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼（前記１０．）を実行すればよい。

【０２０８】

最新のグループ公開鍵に対応したグループ参加証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼（前記１０．）を実行すればよい。

【０２０９】

次に、前記４．で概要を述べたＰ２Ｐネットワークの情報検索の仕組みを利用したグループ情報の取得の処理の流れについて図７を参照して順を追って詳細に説明する。図７はグループの検索を行う検索者Ｘとグループ発行者Ｂでそれぞれ実行される処理の流れを図示したものである。グループの検索が終了したあと、検索者Ｘが保持している情報は図２と同じである。

【０２１０】

［ステップ７０１］

Ｂはグループ管理者から、グループ参加証発行許可証Ｉ＿Ｂ、およびグループ公開鍵ＫＧ＿Ｐを含むグループ情報ＩＧを入手する。

【０２１１】

［ステップ７０２］

検索者Ｘは検索したいグループの条件ＣＧを作成する。このとき指定される条件はグループのカテゴリなどが考えられるが、特に規定されるものではない。ま

た、条件記述の形式も特に限定されるものではない。

【０２１２】

［ステップ７０３］

Ｘは作成したＣＧを含むグループ検索メッセージＭＧ＿Ｑを生成して送信する。この時の送信方法は、ブロードキャスト、マルチキャスト、Ｐ２Ｐネットワークによるメッセージ伝播などを用いて送信されるが、特定の送信方法に限定されるものではない。

【０２１３】

［ステップ７０４］

ＢはグループＭＧ＿Ｑを受け取り、ＭＧ＿Ｑに含まれるＣＧと自分が管理するグループのグループ情報ＩＧとを比較し、自分が管理するグループがＣＧで指定される条件に適合するかを判定する。この判定は管理者が自分で判断しても良いし、プログラムなどで自動的に判定しても良い。ＣＧとＩＧが適合しない場合は、ＢはＭＧ＿Ｑを破棄して処理を終了するか、あるいはＭＧ＿Ｑを別のユーザに送信して処理を終了する。

【０２１４】

［ステップ７０５］

Ｂはグループ公開鍵ＫＧ＿Ｐを含むＩＧ、Ｂのグループ参加証発行許可証Ｉ＿Ｂを含む、グループ情報応答メッセージＭＧ＿Ａを作成する。その後、Ｂの秘密鍵ＫＢ＿Ｓを使用してＭＧ＿Ａに署名を施した後、Ｘに向けて送信する。

【０２１５】

［ステップ７０６］

ＸはＢからのグループ情報応答メッセージＭＧ＿Ａを受け取ると、ＭＧ＿Ａに含まれるＫＧ＿ＰおよびＩ＿Ｂを入手する。

【０２１６】

［ステップ７０７］

ＸはＫＧ＿Ｐを使用して、Ｉ＿Ｂの有効性を確認する。簡単には、ＫＧ＿Ｐを使用して

（１）Ｉ＿Ｂが正常に復号化される、もしくはＩ＿Ｂの署名が確認できる

（２）Ｉ＿Ｂの有効期限が切れていない

の２点を確認することによってＩ＿Ｂの有効性を確認できる。Ｉ＿Ｂの有効性が確認されない場合は、ＭＧ＿Ａは正規の発行者以外によって生成されている可能性があるために、ＸはＭＧ＿Ａを破棄して処理を終了する。

【０２１７】

［ステップ７０８］

ＸはＩ＿ＢからＢの公開鍵ＫＢ＿Ｐを入手する。

【０２１８】

［ステップ７０９］

ＸはＫＢ＿Ｐを使用して、ＭＧ＿Ａの署名の有効性を確認する。署名の有効性が確認されない場合は、ＭＧ＿Ａは第三者によって改竄されている可能性があるために、ＸはＭＧ＿Ａを破棄して処理を終了する。

【０２１９】

［ステップ７１０］

ＸはＡから受信したＭＧ＿Ａに含まれるＩＧを保存する。

【０２２０】

上記の方法を用いることによって、グループの発行者、グループの管理者以外がグループ情報の改竄を行うことを防ぐことができる。

【０２２１】

また、グループを一意に識別する情報にグループ公開鍵を使用することができることは第一の実施の形態におけるグループ情報取得の例で述べた通りである。

【０２２２】

なお、必ずしも管理者がメッセージを生成するのではなく、以前に管理者が生成した応答メッセージを別のユーザがキャッシュしておき応答に使用する実施形態も考えられる。

【０２２３】

次に、前記４．で概要を説明した、Ｐ２Ｐネットワークの情報検索の仕組みを使用したエントリポイントの特定の処理の流れについて図８、図９を参照して順を追って詳細に説明する。図８は検索者Ｘとグループの参加者Ｙでそれぞれ実行

される処理の流れを図示したものである。本実施の形態では参加者Ｙのグループ参加証は、グループ発行者Ｂによって発行されている。図９はエントリポイントの検索が終了した後、検索者Ｘが保持している情報をあらわしている。

【０２２４】

［ステップ８０１］

検索者Ｘはエントリポイントを入手したいグループのグループ公開鍵ＫＧ＿Ｐを含むエントリポイント検索メッセージＭＥ＿Ｑを生成して、送信する。このときの送信方法は、ブロードキャスト、マルチキャスト、ユニキャスト、Ｐ２Ｐネットワークによるメッセージ伝播などで送信されるが、ここでは特定の送信方法を想定していない。

【０２２５】

［ステップ８０２］

ＭＥ＿Ｑを受信した参加者Ｙは、ＭＥ＿Ｑに含まれるＫＧ＿Ｐを入手する。

【０２２６】

［ステップ８０３］

Ｙは自分が参加しているグループの公開鍵ＫＧ＿Ｐ’とＫＧ＿Ｐを比較する。二つの公開鍵が一致しない場合にはＹはＭＥ＿Ｑを破棄して処理を終了する、あるいはＭＥ＿Ｑを別のユーザに送信して処理を終了する。

【０２２７】

［ステップ８０４］

Ｙは自分のグループ参加証Ｃ＿Ｙ、Ｃ＿Ｙを発行したグループ発行者Ｂのグループ参加証発行許可証Ｉ＿ＢおよびＹのエントリポイント情報ＥＹを含むエントリポイント検索応答メッセージＭＥ＿Ａを作成する。ＹはＭＥ＿Ａに対して自身の秘密鍵ＫＹ＿Ｓで署名を行い、署名されたＭＥ＿ＡをＸに送信する。

【０２２８】

［ステップ８０５］

Ｘは受信したＭＥ＿ＡからＩ＿Ｂを取得し、ＫＧ＿Ｐを使用してＩ＿Ｂの有効性を検証する。

【０２２９】

［ステップ８０６］

Ｉ＿Ｂの有効性が確認できない場合、Ｙはグループに属していないとみなされ、ＸはＭＥ＿Ａを破棄して処理を終了する。

【０２３０】

［ステップ８０７］

Ｘは有効性を確認したＩ＿ＢからＢの公開鍵ＫＢ＿Ｐを取得する。同時にＭＥ＿ＡからＣ＿Ｙを取得し、ＫＢ＿Ｐを使用してＣ＿Ｙの有効性を検証する。

【０２３１】

［ステップ８０８］

Ｃ＿Ｙの有効性が確認できない場合、Ｙはグループに属していないとみなされ、ＸはＭＥ＿Ａを破棄して処理を終了する。

【０２３２】

［ステップ８０９］

ＸはＣ＿ＹからＹの公開鍵ＫＹ＿Ｐを取得して、ＭＥ＿Ｑの署名を確認する。

【０２３３】

［ステップ８１０］

署名の正当性が確認されない場合は、ＭＥ＿Ｑは第三者によって改竄されている可能性があるので、ＸはＭＥ＿Ｑを破棄して処理を終了する。

【０２３４】

［ステップ８１１］

ＸはＹをＫＧ＿Ｐによって特定されるグループのメンバであると認定し、ＭＥ＿ＡからＥＹを取得し、グループのエントリポイントとして記憶する。

【０２３５】

上記の方法を用いることによって、グループのメンバ以外がエントリポイント情報を作成したのがグループのメンバであることを確認することができる。

【０２３６】

【発明の効果】

本発明によれば、以下の利点を持つネットワーク上のグループの検索が可能となる。すなわち、

（１）常時稼動しているサーバの運用が不要であり、

（２）検索結果を応答者の秘密鍵、グループ参加証などから生成することにより、グループメンバ以外が検索に対する応答を生成することが出来なくなる。

【０２３７】

これにより、グループのメンバ以外がグループの情報を詐称することを防ぐことができ、サーバがない状況においても、信頼性のある検索を実行することができる。

【図面の簡単な説明】

【図１】

本発明の第一の実施の形態におけるグループの発見の流れを示す図

【図２】

本発明の第一の実施の形態においてグループ情報検索者Ｘが保持する情報を示す図

【図３】

本発明の第一の実施の形態におけるグループのエントリポイント検索の処理の流れを示す図

【図４】

本発明の第一の実施の形態におけるエントリポイント検索者Ｘが保持する情報を示す図

【図５】

本発明の第一の実施の形態における検索に対して、最新のグループ公開鍵を通知する処理の流れを示す図

【図６】

本発明の第一の実施の形態においてエントリポイント検索者Ｘが保持する情報を示す図

【図７】

本発明の第二の実施の形態におけるグループの発見処理の流れを示す図

【図８】

本発明の第二の実施の形態におけるグループのエントリポイント検索の処理の

流れを示す図

【図９】

本発明の第二の実施の形態においてエントリポイント検索者が保持する情報を示す図

【図１０】

Ｐ２Ｐネットワークに参加しているユーザ間での情報転送の流れを表した概念図

【図１１】

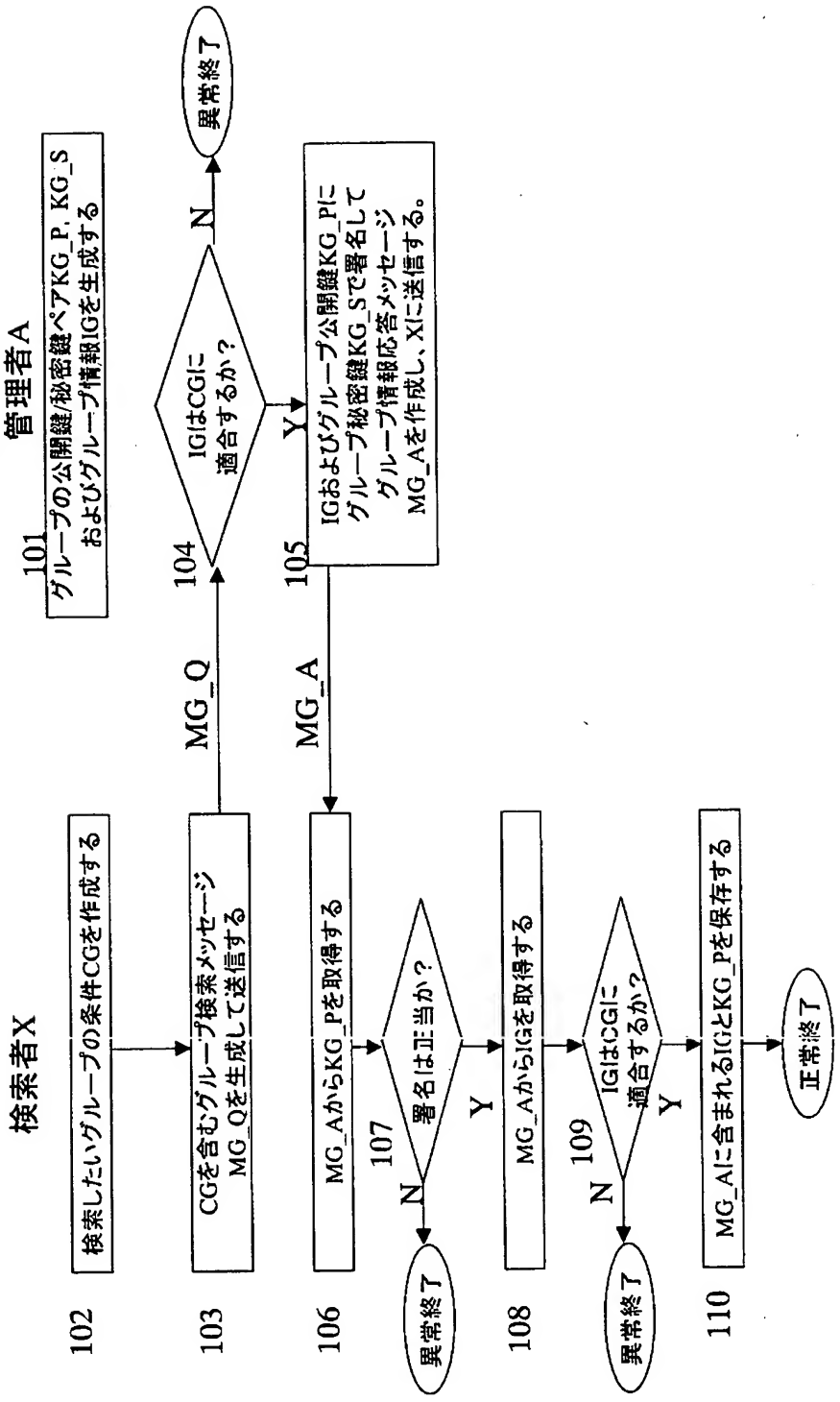
Ｐ２Ｐネットワークにおけるグループ情報検索の流れを表した概念図

【図１２】

Ｐ２Ｐネットワークにおけるグループ情報検索の問題点を図示した概念図

【書類名】　図面

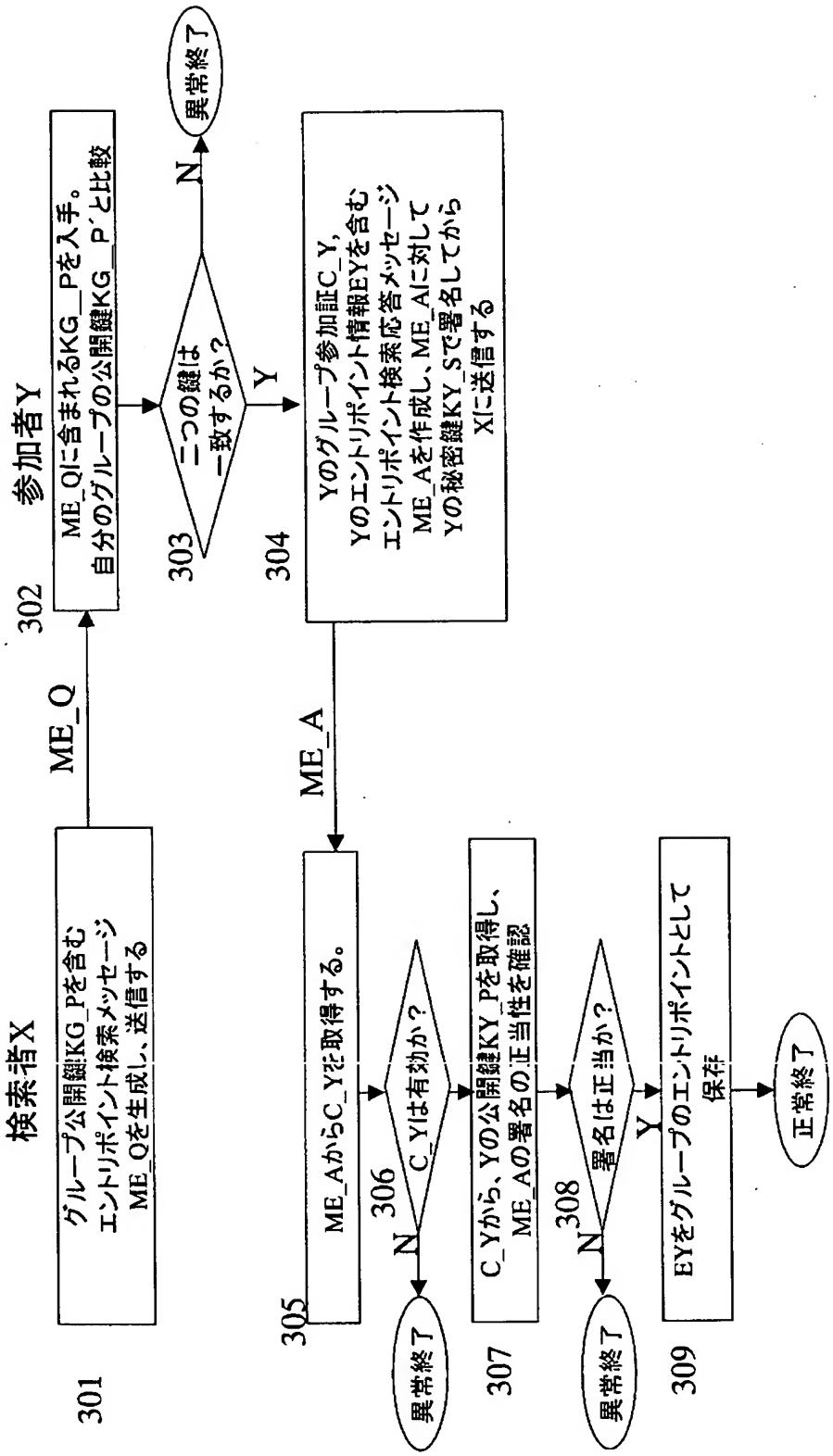
【図１】


管理者A
検索者X
101
グループの公開鍵/秘密鍵ペアKG_P, KG_S
およびグループ情報IGを生成する
102
検索したいグループの条件CGを作成する
103
CGを含むグループ検索メッセージ
MG_Qを生成して送信する
MG_Q
104
IGはCGに
適合するか？
N
異常終了
Y
105
IGおよびグループ公開鍵KG_Pに
グループ秘密鍵KG_Sで署名して
グループ情報応答メッセージ
MG_Aを作成し、Xに送信する。
MG_A
106
MG_AからKG_Pを取得する
107
署名は正当か？
N
異常終了
Y
108
MG_AからIGを取得する
109
IGはCGに
適合するか？
N
異常終了
Y
110
MG_Aに含まれるIGとKG_Pを保存する
正常終了

【図２】

KG_P:グループの公開鍵
IG:グループに関する情報
　（カテゴリや、参加に必要な情報など）

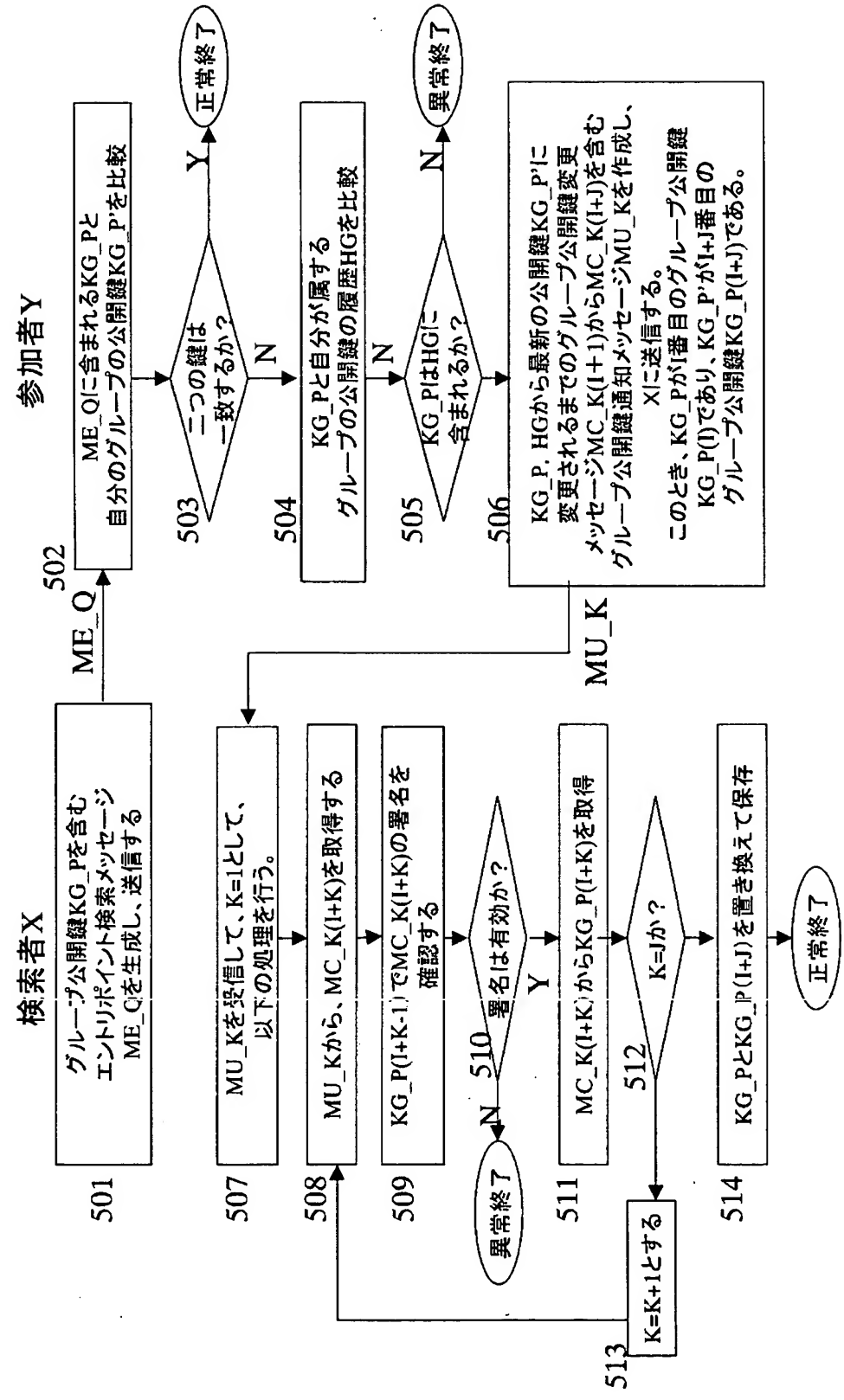
【図３】


検索者X
参加者Y
ME_Q
ME_A
301
グループ公開鍵KG_Pを含む
エントリポイント検索メッセージ
ME_Qを生成し、送信する
302
ME_QIに含まれるKG_Pを入手。
自分のグループの公開鍵KG_P´と比較
303
二つの鍵は
一致するか？
N
異常終了
Y
304
Yのグループ参加証C_Y,
Yのエントリポイント情報EYを含む
エントリポイント検索応答メッセージ
ME_Aを作成し、ME_AIに対して
Yの秘密鍵KY_Sで署名してから
Xに送信する
305
ME_AからC_Yを取得する。
306
C_Yは有効か？
N
異常終了
307
C_Yから、Yの公開鍵KY_Pを取得し、
ME_Aの署名の正当性を確認
308
署名は正当か？
N
異常終了
Y
309
EYをグループのエントリポイントとして
保存
正常終了

【図４】

EY:Yのエントリポイント情報
（IPアドレスやポート番号など）
C_Y:Yのグループ参加証

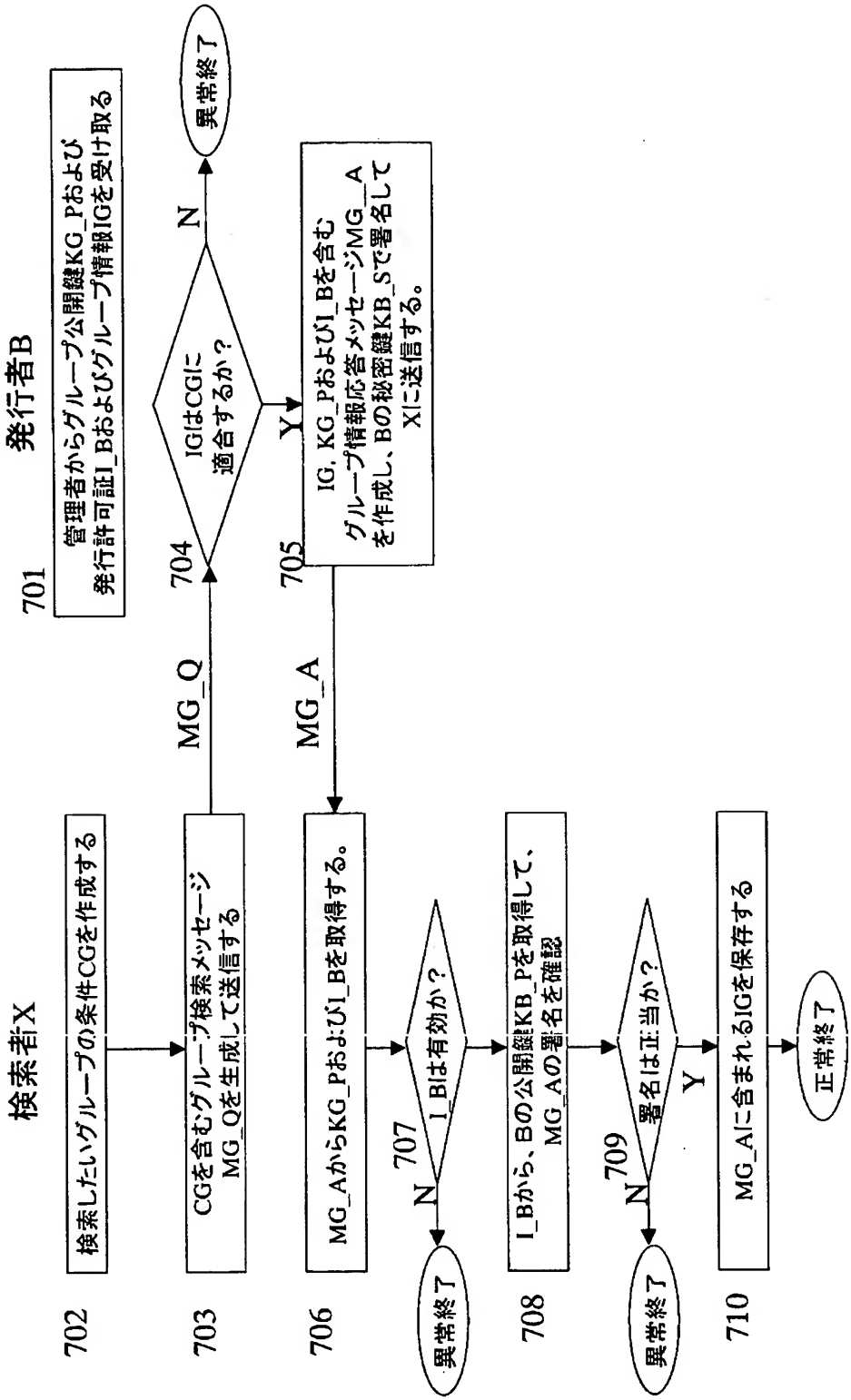
【図５】


参加者Y
検索者X
グループ公開鍵KG_Pを含む
エントリポイント検索メッセージ
ME_Qを生成し、送信する
501
ME_Q
ME_Qに含まれるKG_Pと
自分のグループの公開鍵KG_P'を比較
502
二つの鍵は
一致するか？
503
Y
正常終了
N
KG_Pと自分が属する
グループの公開鍵の履歴HGを比較
504
N
KG_PはHGに
含まれるか？
505
N
異常終了
KG_P, HGから最新の公開鍵KG_P'に
変更されるまでのグループ公開鍵変更
メッセージMC_K(I+1)からMC_K(I+J)を含む
グループ公開鍵通知メッセージMU_Kを作成し、
Xに送信する。
このとき、KG_Pが I番目のグループ公開鍵
KG_P(I)であり、KG_P'がI+J番目の
グループ公開鍵KG_P(I+J)である。
506
MU_K
MU_Kを受信して、K=1として、
以下の処理を行う。
507
MU_Kから、MC_K(I+K)を取得する
508
KG_P(I+K-1)でMC_K(I+K)の署名を
確認する
509
署名は有効か？
510
N
異常終了
Y
MC_K(I+K)からKG_P(I+K)を取得
511
K=J か？
512
K=K+1とする
513
KG_PとKG_P(I+J)を置き換えて保存
514
正常終了

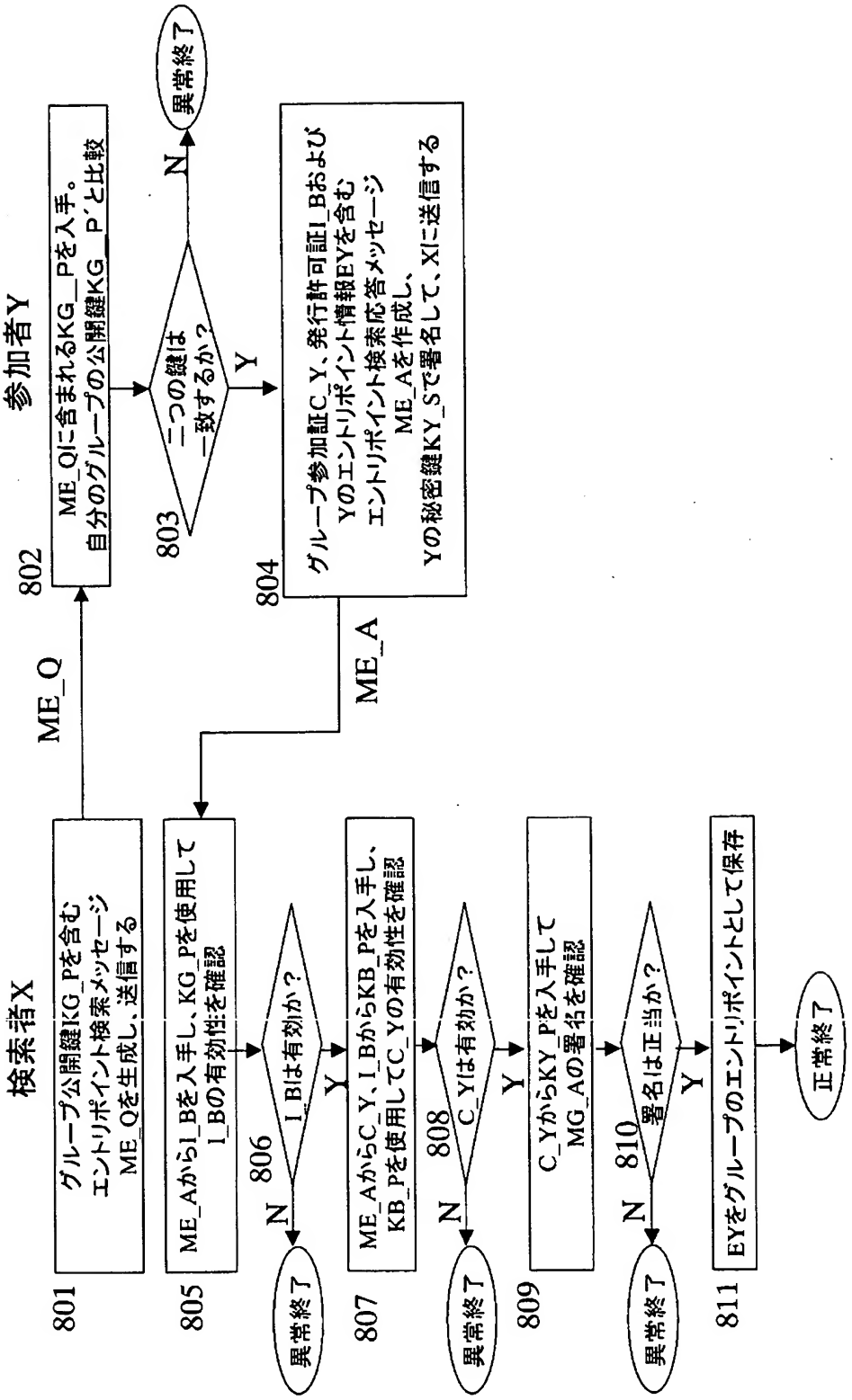
【図６】

KG_P'：最新のグループ公開鍵

【図７】


検索者X
発行者B
701
管理者からグループ公開鍵KG_Pおよび
発行許可証I_Bおよびグループ情報IGを受け取る
702
検索したいグループの条件CGを作成する
703
CGを含むグループ検索メッセージ
MG_Qを生成して送信する
MG_Q
704
IGはCGに
適合するか？
N
異常終了
Y
705
IG, KG_PおよびI_Bを含む
グループ情報応答メッセージMG_A
を作成し、Bの秘密鍵KB_Sで署名して
Xに送信する。
MG_A
706
MG_AからKG_PおよびI_Bを取得する。
707
I_Bは有効か？
N
異常終了
708
I_Bから、Bの公開鍵KB_Pを取得して、
MG_Aの署名を確認
709
署名は正当か？
N
異常終了
Y
710
MG_Aに含まれるIGを保存する
正常終了

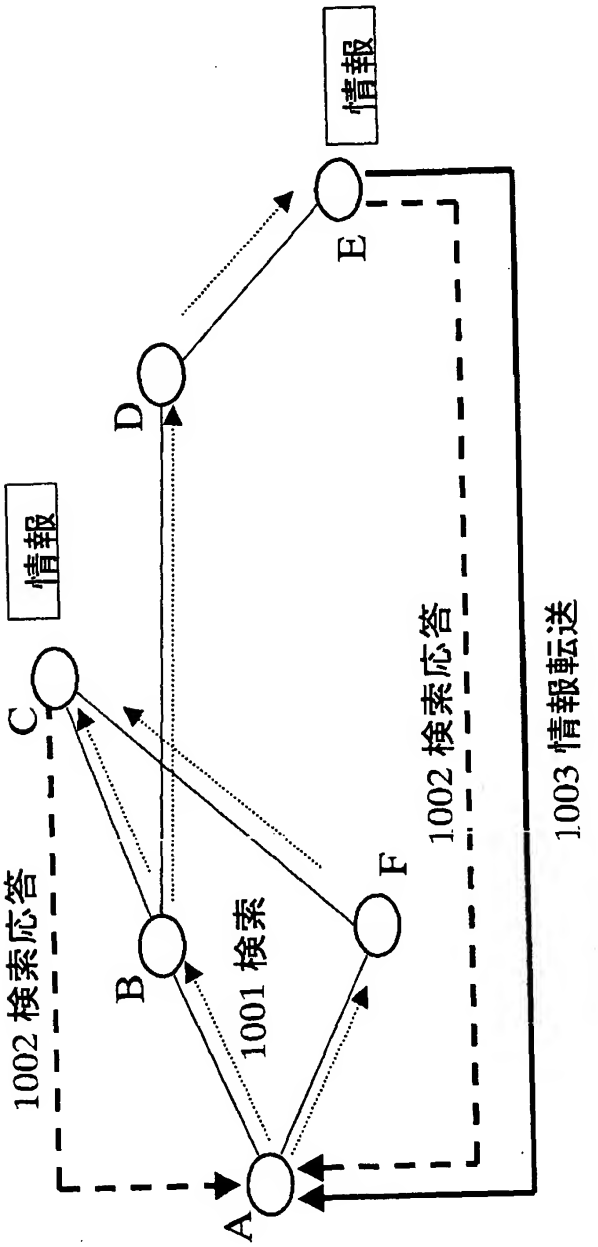
【図８】


検索者X
参加者Y
ME_Q
ME_A
801
グループ公開鍵KG_Pを含む
エントリポイント検索メッセージ
ME_Qを生成し、送信する
802
ME_Qに含まれるKG_Pを入手。
自分のグループの公開鍵KG_P'と比較
803
二つの鍵は
一致するか？
N
異常終了
Y
804
グループ参加証C_Y、発行許可証I_Bおよび
Yのエントリポイント情報EYを含む
エントリポイント検索応答メッセージ
ME_Aを作成し、
Yの秘密鍵KY_Sで署名して、Xに送信する
805
ME_AからI_Bを入手し、KG_Pを使用して
I_Bの有効性を確認
806
I_Bは有効か？
N
異常終了
Y
807
ME_AからC_Y、I_BからKB_Pを入手し、
KB_Pを使用してC_Yの有効性を確認
808
C_Yは有効か？
N
異常終了
Y
809
C_YからKY_Pを入手して
MG_Aの署名を確認
810
署名は正当か？
N
異常終了
Y
811
EYをグループのエントリポイントとして保存
正常終了

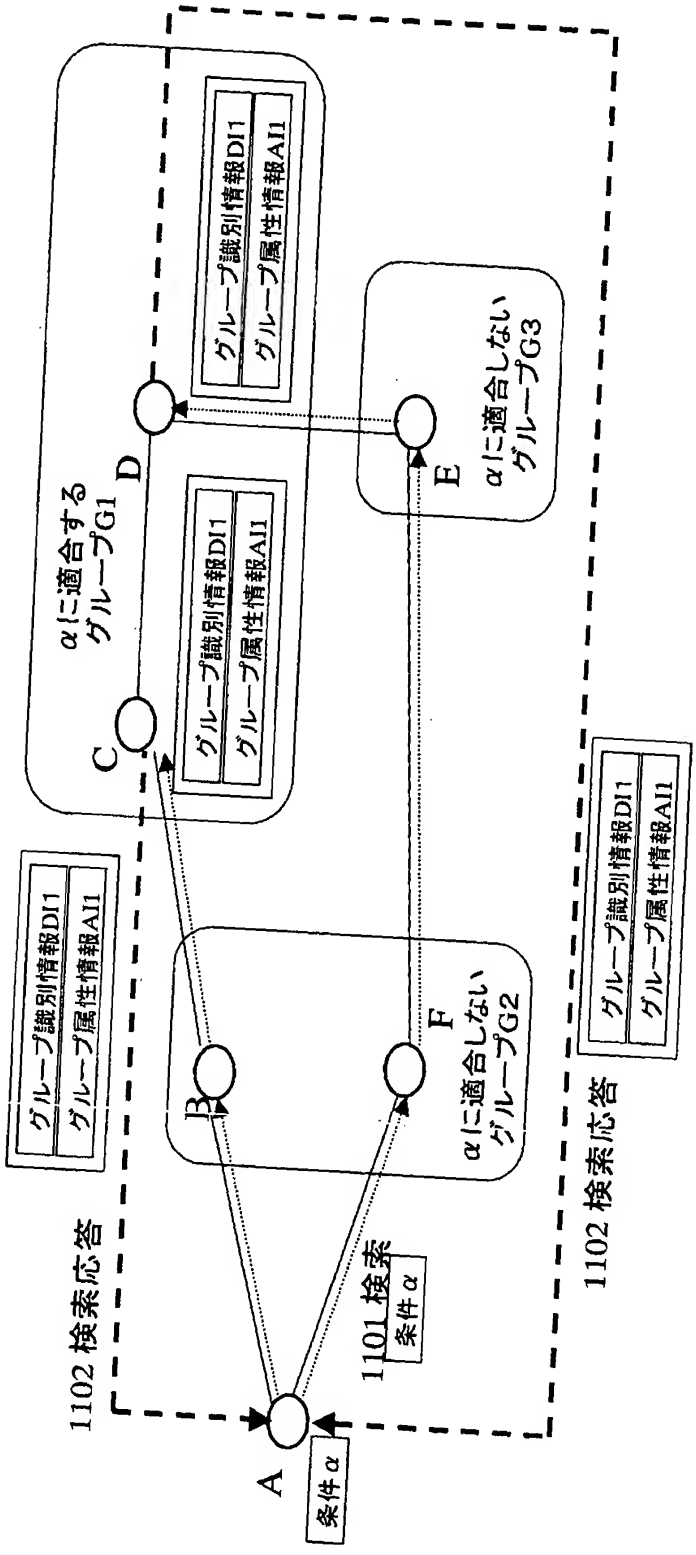
【図９】

EY:Yのエントリポイント情報
（IPアドレスやポート番号など）
C_Y:Yのグループ参加証
I_B:Bのグループ参加証発行許可証

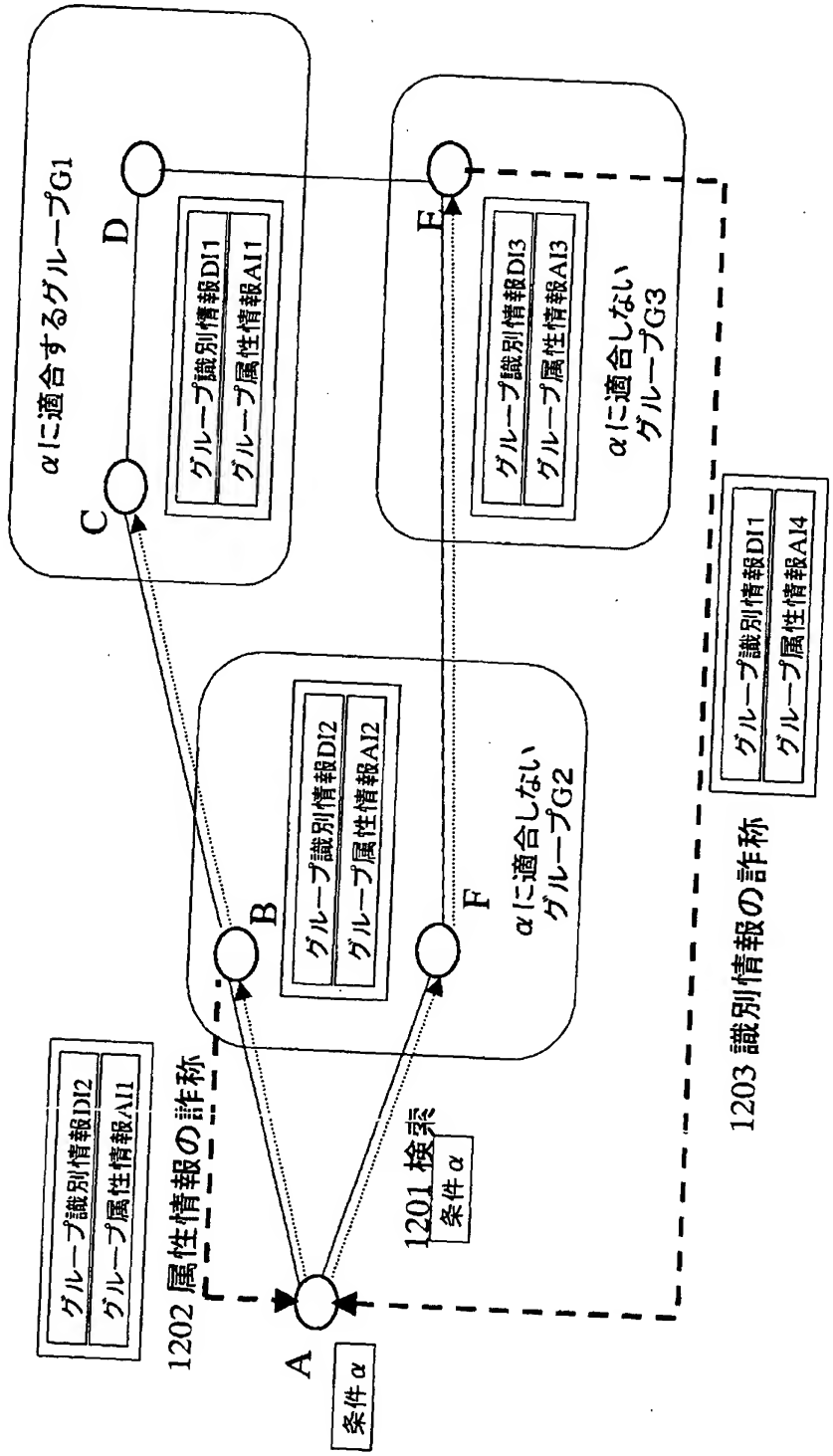
【図１０】



【図１１】


1102 検索応答
1101 検索
条件α
1102 検索応答
A
条件α
B
C
D
E
F
αに適合するグループG1
αに適合しないグループG2
αに適合しないグループG3
グループ識別情報DI1
グループ属性情報AI1
グループ識別情報DI1
グループ属性情報AI1
グループ識別情報DI1
グループ属性情報AI1
グループ識別情報DI1
グループ属性情報AI1

【図１２】


αに適合するグループG1
D
C
グループ識別情報DI1
グループ属性情報AI1
F
αに適合しない
グループG3
グループ識別情報DI3
グループ属性情報AI3
グループ識別情報DI2
グループ属性情報AI2
B
F
αに適合しない
グループG2
グループ識別情報DI1
グループ属性情報AI4
1203 識別情報の詐称
グループ識別情報DI2
グループ属性情報AI1
1202 属性情報の詐称
1201 検索
条件α
A
条件α

【書類名】　要約書

【要約】

【課題】　Peer-to-Peerネットワークでは情報がサーバなどにより、集中管理されていないために、あるグループの情報を第三者が詐称することが容易にできる。

【解決手段】　グループの情報に対する検索に対して、管理者あるいは発行者がグループ秘密鍵もしくは発行者の秘密鍵に基づく応答メッセージを作成する。またグループのエントリポイントに対する検索に対して、グループのメンバが持つ参加証に基づく応答メッセージを作成し、検索応答がグループのメンバからのものであることを保証する仕組みを導入する。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
〔変更理由〕　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社